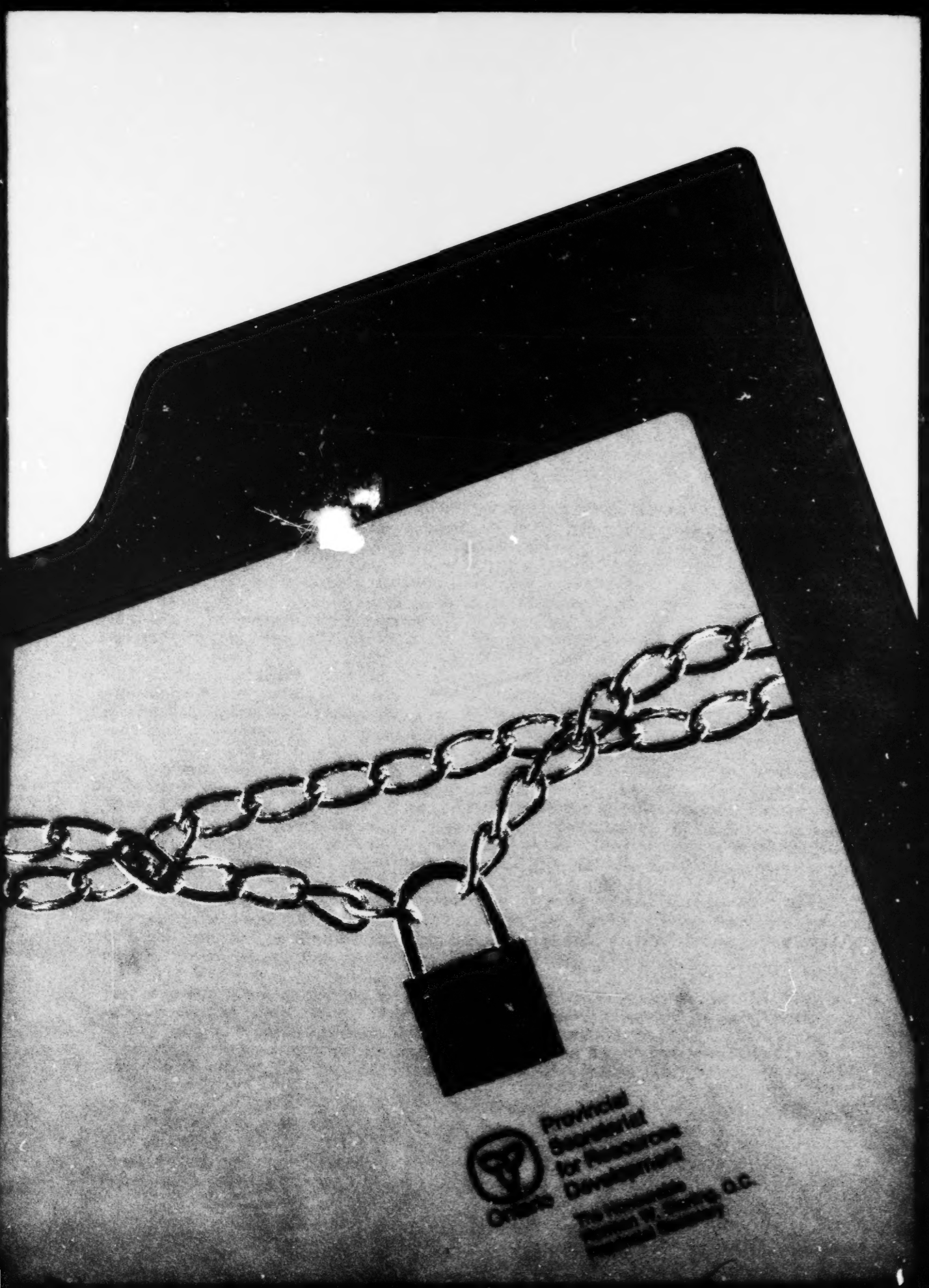
Provincial
Secretariat
for Resource
Development
Provincial Secretariat for Social Development

85-3387/

Ontario

Provincial
Secretary for
Resources
Development

Whitney Block
Queen's Park
Toronto, Ontario
M7A 1A2
416/965-7721

MESSAGE FROM THE MINISTER:

During the last decade, concern for privacy has surfaced as one of the leading issues facing modern industrial societies. This concern has been escalated by technological innovation coupled with the growing awareness that, as citizens, we are no longer in a position where we can rely solely on our own efforts to protect personal privacy.

The right to privacy is something all of us guard closely and value highly. Ironically though, there has never been adequate legal recognition of this right in Canada.

This Discussion Paper examines various options which Governments may wish to consider when developing a response to privacy issues. It is equally important, however, that these concepts be considered in consultation with the private sector.

The importance of developing a uniform approach to this growing issue becomes readily apparent when one realizes that information gathered about an individual may be stored and actually used in another Province or Country.

Some companies in the private sector have responded to privacy concerns by developing privacy codes to govern the handling of personal information in their operations. However, companies with privacy codes are still the exception rather than the norm, suggesting that there is a need to set standards to ensure that infringements of citizens' privacy rights do not occur.

Many European countries presently have some form of Data Protection Legislation in place and, in 1981, the Council of Europe adopted a Data Protection Convention which was signed by all participating countries.

The concerns surrounding privacy and computer protection are very real. It is important, however, that these issues be addressed with industry in a coordinated and responsible manner. It is my hope that this Discussion Paper will serve as a successful first step towards achieving a Privacy Protection Code for citizens.

Norman Sterling

Norman Sterling, Q.C.
Provincial Secretary for
Resources Development

TABLE OF CONTENTS

		Page
Synopsis		iii
PART I:	UNDERSTANDING THE ISSUES	1
	Introduction	1
	Fair Information Practices	4
	Public Perceptions	6
	Industry Response	8
PART II:	LEGISLATION GOVERNING PUBLIC SECTOR DATA BANKS	10
	Canada	10
	Provinces	11
	United States	12
	United Kingdom	13
	Federal Republic of Germany	13
	Sweden	14
	Council of Europe	15
	Organization for Economic Cooperation and Development	15
	Summary	16
PART III:	ALTERNATIVES FOR THE PRIVATE SECTOR	18
	Summary of Issues	18
	Scope	20
	Policy Options	21
	Summary	29

SYNOPSIS

Developments in computer and telecommunications technology have raised new questions about informational privacy - the capacity for individuals to determine what information is collected about them and the manner in which it is made available to others. This Discussion Paper introduces the reader to some of the major issues raised by the potential impact of technological developments on privacy and discusses some alternative approaches to their resolution.

These issues centre on data collection, data quality, disclosure limitations, security safeguards, costs and individual access to personal records in computerized data banks. Recent surveys of public attitudes suggest that individuals are very concerned about computers affecting personal privacy and about institutions collecting too much personal information.

The public sector has begun to address these problems with various statutes which establish and enforce fair information practices for data banks held by government departments and agencies. Examples include Canada's Federal Privacy Act and Quebec's Bill 65, both of which also establish offices to ensure compliance with privacy standards and consider individual complaints regarding information practices.

Ontario is considering a proposal in its draft Privacy and Access to Information Bill that would seek to establish fair information practices for provincial government data banks. It would set up a compliance office as well as an office to receive citizens' complaints regarding information practices.

Data protection has received much attention in Europe, where countries like the United Kingdom, West Germany and Sweden have legislative programs which register data banks and regulate information practices in both the public and private sectors.

The private sector has shown sensitivity to privacy concerns by developing internal practices and, in some cases, voluntary privacy codes which embrace some of the principles commonly found in data protection laws. In the United States, Warner-Amex Cable Communications Inc. has developed a code to protect the privacy of the personal information it gathers on its customers. The Canadian Cable Television Association is in the process of developing a privacy code with similar self-regulation objectives.

Traditionally, credit bureaus, which are regulated in most provinces by credit reporting Acts, have been the main handlers of personal information in the private sector. However, the growth of computerized personal information banks can be seen in a wide range of industries including financial

institutions, cable TV services, videotex services, computer services as well as a host of other business and non-business sectors. The individual has no concrete guarantees against infringements of informational privacy in these data banks.

In order to develop a uniform approach to the privacy problem, Canadian jurisdictions will have to grapple with a number of legal issues. These include questions such as: Who owns the information in personal data banks? How should that information be legally protected? Do existing privacy laws need to be amended in light of the expanding technology? Does liability ensue from an improper or unauthorized release of personal information? Then, of course, there is the everlasting problem of jurisdiction between the federal, provincial and territorial governments to harmonize rules as they are developed and to avoid any conflicts in the laws.

It is a generally held view that individual rights, including privacy rights, are not within the exclusive legislative competence of either the Federal or Provincial levels of government but rather are determined by the Canadian Constitution and more particularly S.91 and S.92 of the B.N.A. Act. Although a number of governments already have Privacy Statutes, it is important that these initiatives continue and perhaps expand.

This paper analyzes four approaches to resolving privacy concerns brought about by the growth in computerized handling of personal information in the private sector. Instead of reviewing the whole spectrum of possible approaches, it focuses on four that are thought to be suitable for the Canadian situation.

The Government has developed a strong role in promoting and adopting microelectronic and communications technology. It therefore has a complementary responsibility to ensure that privacy standards are upheld as the technology is adopted in all sectors of the economy.

The first possible approach would be for government to encourage self-regulation in industries which are important data users. This could take the form of voluntary privacy codes modeled after those used by companies discussed later in this report. The most noteworthy attempts at self regulation also include provisions regarding fair information practices in their customer agreements. Government could work with a representative association in each industry sector in developing a privacy code for that sector. This would produce a series of voluntary privacy codes tailored to fit the requirements of each sector.

A second possibility would be for government to develop legislation which sets out fair information practices and includes a penalty provision for the offense of violating these practices. This could be voluntary in form, covering only those firms which wish to comply, or it could be compulsory, including all important data users in the private sector.

A third possible alternative is to set up a registration and regulation system governing data users. Such a system could set out major principles regarding information handling; set up a Registrar or Commissioner's Office to administer the registration system and ensure compliance with principles; and establish individual rights to access, correction and non-disclosure of personal information. Models of registration systems include the United Kingdom Data Protection Bill as well as systems set up by Canadian provinces to regulate personal credit information.

Combinations of these three approaches would yield other possibilities. One such possibility which is worthy of analysis is a combination of the Self-regulation and Registration approaches described above. For the purposes of this paper, this has been called the "Voluntary Registration" approach. Industry associations could develop privacy codes tailored to their industry, monitor compliance among their members, and mediate complaints from individual citizens. This could be done in consultation with a public Privacy Office which could also keep a registry of all participating associations and companies.

PART I: UNDERSTANDING THE ISSUES

Introduction

The need for informational privacy - the capacity for individuals to determine, in significant measure, what information is collected about them and the manner in which it is made available to others - has long been recognized as a legitimate aspect of a free society. Yet, though the importance of privacy as a value has been widely accepted, its existence has depended in large part on the technological impossibility of detailed surveillance and record-keeping about large numbers of individuals. That technological barrier no longer exists. Therefore, standards will now have to be considered if informational privacy is to be maintained in the face of technological advance.

Key to the creation of such safeguards is the development of a consensus regarding fair information practices. These practices would generally define limits on the way personal information is collected, stored and used. They would also attempt to balance the individual's privacy with competing social values of openness and economic values of efficiency. For the purposes of this paper, personal information may be defined as information in a record about an individual person where that person is identified by name or is readily identifiable by other means.

The purpose of this Discussion Paper is to introduce the reader to the major issues raised by the potential impact of technological developments on individual privacy and to discuss some of the alternative approaches to their resolution.

Recent developments in computer and telecommunications technology have made it possible to process and link information held in a variety of data banks with ease, low cost and speed. In the past quarter century record-keeping by both

government and private entities has moved from the slow, clumsy era of paper files, where information is entered manually, to high speed, efficient, machine-readable files. This development has had a number of significant implications for privacy.

First, machine-readable files are more quickly retrieved and more readily and anonymously updated. What was once a collection of pieces of paper, with the age of each readily apparent, is now a computer readout. Moreover, computer files are easily accessible from many distant points in the organization. More important, however, is the fact that computerized files are readily merged, allowing a number of files dealing with the same subject or individual to be compiled into a single dossier. This can be done within the organization which collected the data. However, data can also be easily transferred to another information user and combined with other files from other sources for uses not envisioned by any of those persons associated with the initial information-gathering process. This is made easier by the use of a single identifying number, but the absence of such a number is not a significant bar to such compilations. In addition, telecommunication links between the holders of files make it possible for the files collected by one institution for one purpose to be shared with other information users for quite different purposes. This process is called data linkage.

The potential impact of efficient retrieval, sharing and merging of files on informational privacy is magnified by the sheer number and variety of sources of computerized information about individuals. The physical size of computers has dropped in twenty years from room-sized machines to ones which fit easily on a desk top. Costs of machinery and processing have dropped at a comparable rate. The older generation of machinery required extensive training to use; present equipment, dubbed "user friendly", can be operated with little specialized training or knowledge.

Where once only the largest institutions, including government, had the resources to effectively use the computer, computerized record keeping is now the norm in virtually every area of human activity. Once the national census was the sole compilation of varied facts about individuals. Now it is possible to compile even more varied information about individuals by the sharing of information among file holders. In government, files held on individuals include information on vital statistics, tax, criminal and court proceedings, health, driving, military and school records, among others.

In the private sector, information held on individuals in computerized files is even more varied. Among the best-known is the credit-rating file. However, the public is becoming aware of other computerized files including those in the insurance, banking and telecommunication industries. In addition, there are many data users of which the public is unaware: retail sellers who have credit card systems or teleshopping services; magazines which keep subscription lists; charitable, business, professional or community organizations; and many other service providers. As cable television companies enter into two-way operations which make it possible for the consumer to undertake telebanking, teleshopping, and instant polling, and order television programs on a "pay per view" basis, greater amounts of personal data will be stored by the private sector.

This all pervasive collection of personal information is a virtually unavoidable feature of life in the last quarter of the twentieth century. As the U.S. Privacy Protection Study Commission concluded in 1977:

> It is now commonplace for an individual to be asked to divulge information about himself for use by unseen strangers who make decisions about him that directly affect his everyday life. Furthermore, because so many of the services offered by organizations are, or have come to be considered, necessities, an individual has little choice but to submit to whatever demands for information about him an organization may make.

Fair Information Practices

This threat to privacy has resulted in a number of attempts to define appropriate limits and to protect the privacy of personal information stored in computer systems. The general principles enunciated in the Council of Europe's "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" are typical of efforts in a number of jurisdictions to establish guidelines which recognize the benefits of computerized record keeping and the value which individuals place on personal privacy. These guidelines include the following concepts:

i) Personal information should be obtained and processed fairly and lawfully;

ii) Personal information should be held for a specified and legitimate purpose or purposes;

iii) Personal information should not be used or disclosed in a way incompatible with those purposes;

iv) Personal information should be adequate, relevant, and not excessive in relation to the specified purposes;

v) Personal information should be accurate and, where necessary, kept up to date;

vi) Personal information should be kept in name linked form for no longer than is necessary for the specified purposes;

vii) The data subject should have access to information held about him or her and be entitled to its correction or erasure where the legal provisions safeguarding personal data have not been complied with;

viii) Appropriate security measures must be taken against unauthorized access, alteration or dissemination, accidental loss and accidental or unauthorized destruction of data.

These guidelines recognize the individual's need to ensure that information which is gathered about him is done so with his consent; that this consent is given with a full and

accurate understanding of the purpose for which the information is gathered; that other uses will not be undertaken without prior consent; that the file will be made available so that the individual can ensure the information is correct; that, in the event there is disagreement about the accuracy of the information, the data subject's version will be noted; and that third parties will not be given access without the individual's knowledge or permission except where required by law.

Even where there is general agreement with these principles in both the public and private sectors, however, there are a number of impediments to their fulfillment. One of these is the companion principle of freedom of information. If an individual has full control over all his personal information, this right can present a major barrier to the rights of others to obtain information on government activities. Clearly a balance must be struck.

Another impediment is the problem of computer crime, where data is taken or released without the permission of the data bank owner. It has been suggested that criminal code amendments which would establish specific offences relating to computer crime would go part way to solving this problem. However, owners of data banks would still have to take reasonable precautions inside their organizations to ensure that personal information is kept confidential and that employees handling this information follow necessary safeguards.

A third potential impediment is the problem of transborder data flow, when information relating to individuals is removed to and processed in another jurisdiction where privacy is not adequately protected by business practices or by law. Here again efficiency and the value of the free flow of information may come into conflict with privacy norms. Certain of these issues are beyond the scope of this discussion since they fall within the realm of the Federal Government.

Public Perceptions

Recent surveys indicate that concerns about privacy brought on by growing computer use are not the sole preserve of academics, futurists, and policy makers. Surveys conducted for the Ontario Government in 1980 and 1983[1] show that a considerable majority of Ontario citizens are concerned about computers affecting personal privacy. In addition, in 1983, about half the population felt that government has the major responsibility for ensuring confidentiality of personal and financial information in our society. An additional 38 percent saw the private sector as having major responsibilities for privacy protection. The earlier 1980 survey further revealed that a sizeable minority believe that institutions such as government, credit-grantors, employers and insurance companies ask individuals for too much personal and financial information.

As well, a 1981 Gallup[2] survey on attitudes toward microelectronic technology asked respondents to indicate the importance of thirteen issues associated with computers and information technology. Privacy and confidentiality of personal information was by far the most important of the issues and was mentioned by 63 percent of the respondents. The number of people controlling information, a closely related issue, was third in importance, mentioned by 45 percent of respondents. Concern for privacy was highest among those who reported that they had knowledge of microelectronics and among respondents who held executive, sales and clerical jobs. Individuals were also asked to look ahead for the next five years and predict whether or not their privacy would be "invaded or seriously disturbed" by any of seventeen organizations, entities, or

---

1. See Ontario Consumer Issues 1980 and Ontario Consumer Issues 1983, Ontario Ministry of Consumer and Commercial Relations.

2. A Gallup Survey of Electronic Technology, March 1981, The Gallup Organization, Inc.

persons. There was a high level of concern. Fifty percent or more of the respondents indicated that they believed that each of the following entities could be the source of an invasion of privacy: a credit rating agency, a computer or data bank, an insurance company, the provincial or federal government, a bank, someone who could interfere with their mail, and someone telephoning them. Again, people who reported knowledge of microelectronic technology were those most likely to anticipate the likelihood of a privacy invasion.

A November 1982 survey conducted in London, Ontario by Professor Neil Vidmar of the University of Western Ontario[3] for the Ontario Government indicated similarly high levels of concern for privacy in the development of interactive services on cable television. Over two-thirds of those surveyed believe that Canadians have less privacy now than ten years ago. The types of information identified as most sensitive and most in need of protection were bank balances, information on when a person enters or leaves his or her home (information collected by home security systems delivered by cable), credit records, personal earnings and medical records. The findings showed that nearly half of the survey respondents were worried about government use of information, but an even greater proportion distrusted private business. Seventy-two percent of the sample favored regulatory intervention by government, with a majority of 52% seeing a regulatory role for both the federal and provincial governments. The study also indicated a widespread belief that many public and private organizations collect more personal information than is necessary.

---

3. Neil Vidmar, Privacy and Two-way Cable Television: A Study of Canadian Public Opinion, University of Western Ontario, 1983.

Industry Response

As the OECD guidelines[4] have noted, one major means to effective privacy protection is the development of self-regulation by industries and firms which make extensive use of personal information. Several firms in this category have responded to the challenge of self-regulation with well-developed internal practices, corresponding to the common definition of fair information practices outlined by the OECD, among others.

Bell Canada, for example, is a major corporation which handles a substantial amount of personal information which is necessarily collected for billing purposes. Company policies consider all subscriber information except name, address and telephone number to be private information held on a need-to-know basis within the company. Personal data are not available for sale, and Bell employees are instructed that all information about customers, wherever collected, is strictly confidential. Indeed the existence, content or nature of any customer communications are not to be made known to third parties, except in compliance with a legal order. Should such an order be made, Bell will notify the customer of the order unless specifically prohibited from doing so.

The Bank of Montreal is another personal data user which has developed and published information on its specific privacy protection practices. Data collected and maintained on file is the minimum necessary for the service desired. Access to that information is strictly controlled within the company, and information is generally not conveyed to third parties without the customer's consent, except that required by stat-

---

4. Organization for Economic Cooperation and Development, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

ute or court order. Customer applications for credit card services, personal loans and mortgage loans, however, include a general consent or waiver clause which authorizes the bank to disclose information about the customer to third parties under certain circumstances. The practice of requiring customers to sign waivers, common among financial institutions, has been criticized in the past as undermining the customer's privacy protection.

Industry-wide self-regulation through establishment of a privacy code is currently being developed by the cable industry in Canada through its association, the Canadian Cable Television Association. A CCTA sub-committee, using the highly regarded Warner-Amex cable privacy code in the United States as a starting point, is in the process of creating a code for the industry tailored to the Canadian situation. It is expected that this code will be accepted and implemented by CCTA member companies as they develop their interactive service offerings. A major advantage of code development prior to the development of services is that systems can be designed in advance to enhance computer security and data protection capabilities.

Companies with voluntary privacy codes are still the exception rather than the norm, however. It is clear, therefore, that the widespread computerized handling of personal information will require the setting of standards in some form to ensure that infringement of citizens' privacy rights do not occur.

PART II: LEGISLATION GOVERNING PUBLIC SECTOR DATA BANKS

There is a growing body of legislation, in Canada and abroad, which addresses itself to the issues surrounding information access and privacy. That most of it is of fairly recent origin reveals the extent to which these issues are interconnected with developing information technologies and the speed with which privacy problems are expected to reach serious proportions. A variety of solutions are in evidence here, some dealing only with the question of privacy as affected by government data banks, others addressing the question of private sector data protection as well.

Canada

Privacy protection on the national level in Canada is focused on development of fair information practices in government data banks under federal jurisdiction. The Canadian Privacy Act, passed in 1982 and proclaimed in 1983, establishes the right of Canadian citizens and permanent residents to know, with certain exceptions, of the existence of information files on them; to examine, correct and challenge information in them; to know to what uses the file has been put; and to be consulted regarding certain future uses thereof. A companion statute, the Access to Information Act, was designed to maximize compatibility between information access and privacy. The Privacy Act requires publication of an annual index to federal information banks, and creates a Privacy Commissioner with the power to mediate disputes, investigate to ensure compliance by the data bank holder in question, and apply to the courts for review of government decisions to withhold information.

Provinces

Both Nova Scotia and New Brunswick have freedom of information legislation dating from the late 1970's. Nova Scotia's lists the types of documents that may be accessed, rather than establishing a general access principle, while the New Brunswick Act establishes general principles, with appeals to an ombudsman and in camera inspection by the courts of contested documents.

Newfoundland passed both Freedom of Information and Privacy Acts in 1981. The former lists the departments, boards, agencies and commissions affected, while the latter makes it "a tort, actionable without proof of damage, for a person...to violate the privacy of an individual."

Quebec deals with freedom of information and privacy together in an Act passed in 1982 and designed, like the federal Act, to protect personal information in government files, while allowing access to documents of public bodies. These bodies include not only the provincial government and all its departments and agencies, but also municipalities (including county, regional and city governments and agencies), and educational, health and social service institutions. The Act requires that an index of files kept by public bodies be compiled for circulation by The Information Access Commission and that requests for information be processed free of charge and within twenty days of receipt. The Commission has a variety of supervisory, investigatory and decision-making powers.

Ontario has examined the questions of privacy and access to information extensively in the past. As a result it has been proposed, in Ontario's Privacy and Access to Information Bill, that fair information practices be defined and made obligatory for government data banks. The proposal would establish a Data Protection Office with authority to develop and apply standards for the management of personal data systems. These standards would include requirements to restrict

information collection to the minimum essential for the operation of a program; provide that personal information normally be collected directly from its subject, and that the reason for its collection be disclosed; and generally require that information collected not be disclosed without the individual's consent. Exceptions to the rule of authorized disclosure include occasions where it would not represent an unwarranted invasion of personal privacy, where it is necessary for the administration of authorized government programs, or where it is in the best interests of the individual or society. Individuals would also have the right to access and correction of files, with the data holder obligated to notify past users of the file of any correction. Individuals would also have the right to file complaints to a separate Commissioner's office.

In 1968 British Columbia passed The Privacy Act and became the first Commonwealth jurisdiction to establish an independent cause of action for the unreasonable and unwarranted invasion of an individual's privacy. This Act was followed by similar legislation in Manitoba and Saskatchewan. None of these privacy Acts, however, deal expressly with the inappropriate or unauthorized use of personal information which has been given voluntarily to another person or institution and integrated into an information bank. Moreover, there is a strong financial disincentive to the individual in enforcing his or her rights through the courts, since the costs of the action would often outweigh potential benefits.

United States

The United States' Privacy Act dates from 1974 and applies to personal information held in government records. It is essentially a "good housekeeping" statute which sets standards for administration of data files. As such, it requires government to report regarding the existence of information files, to ensure the quality of the information therein, to provide access to the subjects of such files, to use data only

for the purposes for which it was collected, and to provide a record of disclosures of that information to the individual affected. There are no time limits for response, and the Act is self-enforcing in that the individual affected has recourse to the courts rather than a separate authority. The United States also has a Freedom of Information Act with rather wider rights of access than the Privacy Act.

United Kingdom

Parliament is now in the process of considering data protection legislation which encompasses both private and public sector automated data banks. It establishes a Data Protection Registrar and Tribunal; requires that both private and public data banks be registered (with certain exceptions); prohibits unauthorized disclosure of information; provides access for individuals to data in registered data banks; and entitles them to amend files and to seek compensation in the courts for damages suffered. The Registrar is empowered to de-register data banks which contravene data protection principles and can prohibit the transfer of data outside the United Kingdom where the country of destination fails to meet minimum data protection standards. This legislation will enable the United Kingdom to adhere to the Council of Europe Convention on data protection.

Federal Republic of Germany

While there is no general access to information law, the Federal Republic of Germany has a highly developed network of data protection arrangements aimed at safeguarding personal privacy. These include both the Federal Data Protection Act and state data protection legislation, which enshrine in law the data protection principles of the Council of Europe. The Federal Act covers both federal public sector data banks and the private sector on a nationwide basis, while state Acts

each govern their respective government's data practices. Primary responsibility for ensuring that the laws are followed falls on the heads of government agencies which create and use personal information files. As well, both Federal and state legislation provide for the establishment of the office of Data Protection Commissioner, with responsibility to supervise and advise agencies which handle personal data and to report to the legislature annually. The success of this system of data protection lies not in the coercive powers available to the Data Commission, but on the high degree of consciousness of appropriate data handling procedures which has been achieved both in the public and in government.

Sweden

Sweden has been the world leader in both access to information and data protection legislation. Access to government information is regulated by the Freedom of the Press Act and the Secrecy Act, which taken together, provide access within a set of specific and limited exceptions. Information privacy is provided through several legislative Acts, the most important of which is the Data Act of 1973. This Act created a Data Inspection Board to regulate the collection and use of personal data in computerized form in both the public and private sectors. Thus the major function of the Board is the licensing of all data registers held by government or private sector data users, and the setting of the rules which govern their use. Decisions of the Board can be appealed to the Minister of Justice and to Cabinet, though the number of such appeals has consistently been small. In general, the first priority of the system is the protection of personal privacy, with less weight given to economy and efficiency in data use.

Council of Europe

The Council of Europe has prepared a "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" which has as its purpose the securing of respect for the individual's right to informational privacy. It requires signatory states to give effect in domestic law to the basic principles for data protection embodied in the Convention. These include: fair information gathering practices; limitations on use and contents of files in light of the purposes for which they were gathered; accuracy; minimal identification of individuals; limitations on the kinds of data to be processed; appropriate security measures; and procedures for identification, examination and correction of files by the individual to whom they pertain. It also confirms the right of signatory states to refuse to allow personal information to be sent to countries without comparable data protection provisions.

Organization for Economic Cooperation and Development (OECD)

The Council of the OECD has developed guidelines governing the protection of privacy, which it regards as minimum standards for its members. In a manner similar to the Convention of the Council of Europe, the OECD subscribes to the following principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability. While specifically noting that data protection should not provide an excuse for restriction of transborder data flow, the OECD agrees that member countries should prevent the export of data which circumvents domestic privacy legislation, or involves export of data to countries not substantially observing the OECD principles. In particular, member countries are urged to: adopt appropriate domestic legislation; encourage and support self-regulation; provide reasonable means for individuals to exercise their rights; provide adequate sanctions;

and ensure that there is no unfair discrimination against data subjects.

Summary

The preceding discussion suggests that the privacy legislation in these various jurisdictions covers a wide spectrum. Most laws ascribe to a similar set of fair information practices or principles. Although there is some variation on finer points, such as whether or not information collected must be "relevant" and collected "directly", most laws establish individual rights to access and correction, and build in some controls over the transfer of personal information to third parties. However, beyond this basic similarity, these laws vary greatly in their strength and application.

For the purposes of this paper, it is worth noting three of the models discussed above. The United States Privacy Act, at one end of the spectrum, provides an example of a self-enforcing law which sets out certain individual rights but does not establish a separate enforcement agency. The Act leaves it up to the individual to seek recourse through the courts.

A second model, illustrated by the Canadian Privacy Act, establishes an enforcement agency with investigation and monitoring responsibilities. Aggrieved individuals can complain to the Privacy Commissioner who can also apply to the courts for review of government decisions to withhold information. The new Quebec law has some similarities, although it has wider application, covering municipalities, school boards, universities and health and social service agencies as well as government departments. The Quebec law gives its Commission significant powers to supervise information practices, respond to complaints, conduct investigations, and issue binding orders to a public body.

A third model that could be identified on this spectrum is illustrated by the United Kingdom registration system described above. In some ways this system of regulation is stronger than the two models summarized above because it requires the formal registration of data banks and gives the Registrar substantial powers of investigation and enforcement, including the power to refuse registration of data banks if the user does not comply with the principles of the Act. The Swedish and German registration systems go further and could be regarded as two additional models on this spectrum.

PART III: ALTERNATIVES FOR THE PRIVATE SECTOR

Summary of Issues

The first part of this paper has discussed the challenge which computerized handling of personal information poses for the protection of privacy. From this discussion emerge a number of competing notions. Most would agree that there is a need to weigh the gains in computer efficiency and speed against the costs to individual privacy which have arisen. In economic terms, therefore, there are conflicting pressures for business establishments to achieve all the cost savings new technology has to offer on the one hand, and to provide the individual with reasonable privacy protection, on the other.

Although it is difficult to generalize, the cost of providing minimum privacy protection is thought not to be great in relation to the efficiency savings usually afforded by new technology. Moreover, these "protection" costs are often minimized if standards or procedures are established prior to the introduction of new systems.

The privacy issues outlined in Part I could be summarized as follows:

1) Data Collection: Should personal information collected by data users[5] be limited to that which is relevant to the user's specified purpose and to that which has received the data subject's informed consent? Should there be a further requirement that personal information be

---

5. The following definitions are used in this section:
Date User: Institution which collects and handles personal information on individuals.
Data Subject: Individual who is the subject of data collection.

collected directly from the data subject? The major statements of principle on the data collection issue usually also include a reference to data being obtained fairly and lawfully for a legitimate purpose. This paper assumes that legitimacy is not at issue and will focus on relevance and informed consent with regard to data collection.

2) Data Quality: Should personal information collected by data users be subject to a requirement to be accurate, complete and up-to-date?

3) Disclosure Limitations: Should disclosure of personal information by data users to third parties be limited to only that information required to fulfill the user's specified purpose? Exceptions would include cases where the subject consents or where disclosure is compelled by law.

4) Security Safeguards: Should data users be subject to a requirement to ensure the physical security of personal records?

5) Individual Access: Should data subjects have the right to confirm the existence of their personal data in records, inspect and receive copies of the data, and request changes to erroneous or incomplete data?

6) Costs: If citizens are given rights of access, correction and non-disclosure, the cost of enforcing these rights must not be prohibitive. Regulatory options which give enforcement agencies quasi-judicial powers to settle grievances may present one option for providing enforceable rights for individuals.

This section will analyze a number of alternative solutions to these issues as they apply to the private sector and then review the strengths and weaknesses of each alternative. The analysis begins with the assumption that the need for informational privacy is a legitimate claim and that the principles enunciated by the Council of Europe's Convention on Data Protection (summarized on page 4) represent a reasonable list with which to evaluate policy alternatives in this area.

Scope

This paper attempts to deal with both the public and private sectors. From the individual citizen's point of view, the threat to privacy of personal information exists in both sectors. Although North American privacy laws have thus far only addressed the problem in the public sector, countries like the United Kingdom[6], West Germany and Sweden have legislative programs in place which cover both sectors.

This leads to the question of self-regulation or government regulation. Some of the competing arguments concerning the effectiveness and desirability of self-regulation as a means of ensuring fair information practices will be examined below in the context of the private sector.

Another general question which all jurisdictions have to decide is whether regulatory programs should cover only computerized personal records or whether they should apply to all personal records, manual and computerized. The major premise in the United Kingdom's White Paper[7] on data protection is that computerization presents new threats to privacy because

---

6. At the time this report was written the U.K. Bill had passed Second Reading.

7. Data Protection: The Government's Proposals for Legislation, Home Office, United Kingdom, April 1982.

of the speed, low cost and ease with which personal information can now be distributed. The implication here is that the costs and effort involved in the transferring of information in manual files act as a disincentive to unauthorized disclosure.

On the other hand, the data protection laws covering public sector records in North American jurisdictions do not distinguish between computerized and manual records. These laws provide the individual with certain rights regarding personal information in both computerized and manual records. The importance of manual records is seen when categories such as health information are considered.

Another important question is whether all data banks, or only those above a threshold size, should be covered by whatever regulatory or self-regulatory approach is undertaken. It is argued by some that only those data users above a threshold size should be candidates for regulation, since the cost of compliance is a greater burden for smaller institutions. However, exemption of smaller data banks would leave information in those banks unprotected, thereby weakening individual rights.

Policy Options

This section looks at four possible options: a voluntary privacy code, a legislated code, a registration and regulation system, as well as an approach which combines elements of the first three. This list is not intended to be exhaustive, but to offer for discussion some reasonable alternatives which could fit the Canadian situation.

1) Voluntary Privacy Code: If the need for privacy protection is accepted as a legitimate claim, governments could encourage specific industries (through their associations) and corporations which are important data users to develop

voluntary codes, incorporating the important principles normally embodied in data protection laws. Companies such as Warner-Amex in the U.S. and IBM in Europe have already developed guidelines for the protection of personal information in their files. In Canada, the Canadian Cable Television Association is in the process of developing a privacy code.

In 1981, Warner-Amex Cable Communications Inc. developed a code designed to protect the privacy of personal information which the company compiles on individual subscribers of cable TV services. In the code, the Company agrees to keep subscriber information physically secure and confidential and agrees to keep subscribers informed of all information gathering functions of the cable TV services being provided. Agreements with individual subscribers set out the terms under which information will be used and provide that no other individual data will be collected without the individual's consent. The code also gives the subscriber the right to examine his or her file and request corrections of erroneous data.

The code is being made a part of subscriber contracts and franchise agreements, making it self-enforcing and giving the subscriber certain rights by agreement. In theory, an individual who felt that his privacy rights had been infringed could commence a civil legal action for breach of contract.

Comments: The advantages and disadvantages of the voluntary code approach as a resolution to privacy issues could be summarized as follows:

- It provides no assurance that the majority of important data users will voluntarily adopt codes.
- No formal enforcement or compliance methods are established (except the limited power of the individual to seek recourse for breach of contract, in cases where the code is supplemented by a written agreement between data user and subject).

- It imposes the least cost and interference on data users.
- It features maximum flexibility, since codes could adapt to changing technology and public requirements.
- It does not guarantee substantial rights for individuals in the case of a dispute over access, correction or disclosure.
- The adoption of various voluntary codes by different industry sectors and companies would result in a lack of uniformity of privacy protection for individuals.

2) Legislated Privacy Code: One approach which falls in between voluntary codes and more traditional government regulatory solutions, consists of developing legislation which would set out fair information practices and would include a penalty provision for the offense of violating these practices. Fair information practices could cover the issues of data collection and quality, disclosure limitations, security safeguards and individual access as set out above. This law would permit a civil lawsuit in tort and would essentially constitute a self-regulatory approach to the problem since it would not require the establishment of an enforcement agency.

Some authors have suggested that public demands for privacy rights have arisen from the failure of legislatures and courts to develop such a body of law[8]. It is generally agreed that the common law in Commonwealth countries offers no protection for personal privacy per se.

---

8. For example, see Roger Noll, "Regulation and Computer Services", in M. Dertouzos and J. Moses, The Computer Age: A Twenty-Year Review, (Cambridge: MIT Press, 1980) and Murray Rankin, Privacy and Technology: A Canadian Perspective (Canadian Institute for Legal Studies, Cambridge University, 1983).

The Privacy Acts enacted by British Columbia, Saskatchewan and Manitoba have been used infrequently and are also thought not to provide the individual with substantial remedies for the types of privacy problems brought on by the computerized handling of personal information.

Legislation establishing a privacy code could take one of two forms:

(a) An Act could permit voluntary compliance. Regulations to the Act could register those industries or companies which wish to comply. Voluntary participants would thus be identified as privacy-conscious companies in their field.

(b) Alternatively, an Act could require compliance. It could apply to all data users, or only to those institutions with data banks above a threshold size.

Comments: Following is a summary of the strengths and weaknesses of this approach:

- It provides no assurance that a majority of data users would voluntarily comply. Only the compulsory version of such a statute would guarantee participation by a majority of data users.
- The remedy available to the individual is costly and impractical. It would likely not be used often since the cost to the individual would almost always exceed possible benefits from using this remedy. Therefore, this approach also does not provide substantial rights to individuals regarding access, correction, disclosure and resolution of disputes.
- It imposes little cost and interference on data users.
- It allows a high degree of flexibility, since the legislation would phrase fair information practices

in general terms, thereby not hampering the application of new technology.

- If remedies were not used widely by individuals, such an Act would not have a major effect on information practices. The compulsory version of such an Act, however, might encourage some uniformity in general data collection and disclosure practices.

3. Registration and Regulation: Another possible solution to these issues is for government to legislate to require registration of data banks; give individuals defined rights of access and correction; regulate the collection and third-party disclosure of personal information; guarantee the security of data and establish a Registrar with investigation and enforcement responsibilities. The registration requirement could apply to those institutions which automatically process personal information in data banks.

This is basically the approach taken by the United Kingdom in their Data Protection Bill, referred to in Part II of this paper. This Bill sets out a registration and enforcement system covering data users which process personal information automatically. Although it applies to both the public and private sectors, the basic structure of this registration system can serve as a useful model for our discussion purposes here.

In this model, the public registry of data users helps individuals become aware of the existence and purpose of computerized personal information banks. The data user is required to identify himself, the information he uses, where it has come from and to whom it is disclosed, as well as the purposes for which it is used. The Registrar has the power to make inquires, to inspect data files and to require modifications to a system. In extreme cases, he may refuse registration for non-compliance with the major data protection principles embodied in the Act. Since the Registrar is given such

wide powers, the Bill sets up an appeal process to an independent tribunal, composed of judicial and computer experts.

The United Kingdom Bill also gives the individual rights of access to personal data; the right to compensation for damages from use of inaccurate data, loss of data and unauthorized disclosure; as well as the right to apply to the courts for rectification or erasure of incorrect data. The individual would have to apply to the court if a data user contravenes any of these individual rights, in order to secure compliance or seek damages in civil proceedings.

Other features of the Bill enable the Government to restrict the transfer of categories of information to specified countries which do not have data protection legislation of comparable strength; give the power to make regulations governing particular categories of personal data such as racial origin, political and religious beliefs; and exempt the collection of data for research purposes where individuals are not identifiable.

The following comments focus only on the general characteristics of a registration system such as the one modeled in the United Kingdom Bill as they could apply to the private sector. They are not meant as an evaluation of the Bill overall.

Comments: The advantages and disadvantages of this approach could be summarized as follows:

- It provides legislated privacy protection covering all important data users and includes an enforcement mechanism to ensure compliance.
- It provides the individual with legal rights of access and correction as well as protection against disclosure to third parties. However, the enforcement of these rights in the case of a dispute may be

costly to the individual since the remedy involves application to the courts.

- This approach imposes new regulation on the private sector, resulting in additional costs for data users.
- It allows some flexibility, since the data protection principles are general and the Registrar's powers are defined broadly, allowing him to handle demands of changing technology and information practices.
- It would have a major impact on information practices because of the registration and enforcement powers.

Registration schemes are a common feature of data protection legislation in other European countries. Brief descriptions of the legislation in West Germany and Sweden, probably the other two most noteworthy examples, are given in Part II.

The major disadvantage of this model from the citizen's point of view is the cost of enforcing his rights through the courts. An alternative model of a registration system could build in the possibility of an appeal from the citizen to a registrar or commissioner who would have the power to issue binding orders affecting the data user. This would remove the cost disincentive for the individual.

Many Canadian provinces regulate the collection and disclosure of personal credit information through credit reporting Acts. In Ontario, for example, the Consumer Reporting Act registers credit bureaus, regulates the gathering, storage and disclosure of credit information, and gives the individual access to his or her personal credit file. The Registrar has the power to revoke or refuse registration under certain circumstances, in which case the applicant is entitled to an appeal to a tribunal. The models used by provinces to regulate

credit information might also provide some guidance to registration systems contemplated for personal data users.

4. Voluntary Registration: Combinations of the above three approaches could produce other possibilities. One such possibility which is worthy of analysis is a combination of the Self-Regulation and Registration approaches described above. Industry associations could develop privacy codes tailored to their industry, monitor compliance among their members, and mediate complaints from individual citizens. This could be done in consultation with a public Privacy Office which could also keep a registry of all participating associations and companies.

Comments: Following is a summary of the strengths and weaknesses of this approach:

- As in the self-regulation model, this solution offers no assurance that the majority of data users will voluntarily join a registration system.
- It would establish a monitoring system to encourage compliance by participating companies and agencies. Although this could be a very positive force, no formal compliance or enforcement powers would be available.
- It would result in some extra costs to data users.
- It features a great degree of flexibility allowing industry and the coordinating agency to respond to changing technology and information practices.
- It does not guarantee concrete rights for individuals in the case of a dispute over access, correction or disclosure. The complaint handling activities of industry associations, however, could fulfill a mediation role.
- Although the adoption of different privacy codes by different industry sectors would result in some differences in privacy standards across the economy,

the coordinating agency could work for uniformity on important issues such as the individual's rights to access, correction and non-disclosure.

Summary

This section has attempted to compare the effectiveness of several alternative methods of resolving informational privacy issues in the private sector. Rather than reviewing all the possible approaches, including more stringent government registration and licencing schemes, this paper has focused on those approaches which are thought to be more suitable to the Canadian situation.

The table on the following page contains a comparative summary of the four approaches outlined above. The criteria used for comparison are based on the preceding analysis and reflect the major consideration central to any discussion of regulatory options: the balance between cost to industry and the provision of individual rights or protections to citizens. Terms in the table, such as "Low/Medium/High" are used to suggest relative values only.

EVALUATION OF ALTERNATIVE SOLUTIONS

	ALTERNATIVES			
BASIC CRITERIA	VOLUNTARY PRIVACY CODES	LEGISLATED PRIVACY CODES	REGISTRATION AND REGULATION	VOLUNTARY REGISTRATION
Cost of Compliance to Data User	Minimum	Minimum	Moderate to High	Moderate
Flexibility	Maximum	Moderate	Moderate	Maximum
Individual Rights to Access,Correction and Non-Disclosure	No Guarantee	Legislated rights under compulsory version of such a law	Establishes Legal Rights for Individuals	No Guarantee
Individual Rights in Dispute Resolution	None	Costly and difficult for individual to enforce	Costly for Individual to Enforce (Alternative registration systems could remove cost burden on individuals)	None
Uniformity of Information Practices	Difficult to Achieve	Possible under compulsory verison of such a law	Registration Encourages Uniformity	Some Uniformity Possible
Effectiveness in Developing Overall Standards for Privacy	Low to Medium	Low to Medium	High Potential	Medium

DOCUMENT: 870-123/004

CONFÉRENCE INTERPROVINCIALE SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS : MESURES POUR 1984 (COLLOQUE)

Document de travail sur la vie privée:

Projets pour 1984

Ontario

Toronto (Ontario)
Les 23 et 24 mai 1984

Ontario

Secrétaire
provincial au
Développement
des ressources

Édifice Whitney
Queen's Park
Toronto (Ontario)
M7A 1A2
416/965-7721

MESSAGE DU MINISTRE :

Au cours de la dernière décennie, la protection de la vie privée a posé un problème majeur aux sociétés industrielle modernes. L'inquiétude est allée croissant à mesure que les citoyens se rendaient compte que le bouleversement technologique était tel qu'ils ne pouvaient compter sur leurs seuls efforts pour protéger les renseignements personnels les concernant.

La protection de notre vie privée est un droit auquel nous tenons tous et qui doit être respecté à tout prix. Aussi étrange que cela puisse paraître, ce droit n'a jamais été reconnu officiellement au Canada.

On trouvera dans ce document de travail un choix de propositions que les gouvernements qui cherchent une solution à ce problème pourront examiner. Il est également important que ces questions fassent l'objet d'une consultation avec le secteur privé.

Il est d'autant plus nécessaire, en effet, de répondre de façon uniforme aux préoccupations que suscite cette question que l'on prend davantage conscience du fait que les données recueillies sur un particulier peuvent être conservées et, en fait, utilisées dans une autre province ou un autre pays.

Dans le secteur privé, certaines compagnies ont réagi en soumettant la manipulation des renseignements personnels à des codes visant à protéger leur caractère confidentiel. Les compagnies qui utilisent ce type de code sont cependant davantage l'exception que la règle et il semble qu'il soit nécessaire d'établir des normes pour empêcher toute ingérence dans le droit des citoyens à la protection de leur vie privée.

De nombreux pays d'Europe ont mis en place des lois sur la protection des données personnelles et, en 1981, le Conseil de l'Europe a adopté une convention de protection des données signée par tous les pays participants.

Les inquiétudes suscitées par le droit à la protection des renseignements sur ordinateurs sont très réelles et il est essentiel d'aborder le problème de façon responsable, en collaboration avec l'industrie. J'espère que ce document de travail constituera un premier pas important vers l'élaboration d'un code de protection de la vie privée des citoyens.

Le Secrétaire provincial
au Développement des ressources

Norman Sterling

Norman Sterling, c.r.

TABLE DES MATIÈRES

		Page
Synopsis		iii
PARTIE I :	COMPRENDRE LES PROBLÈMES	1
	Introduction	1
	Pratiques loyales en matière d'information	4
	Perceptions du public	7
	Réponse du secteur privé	9
PARTIE II :	LOIS RÉGISSANT LES BANQUES DE DONNÉES DU SECTEUR PUBLIC	11
	Canada	11
	Provinces	12
	États-Unis	14
	Royaume-Uni	14
	République fédérale de l'Allemagne occidentale	15
	Suède	16
	Conseil de l'Europe	16
	Organisation pour la coopération et le développement économique	17
	Résumé	17
PARTIE III :	SOLUTIONS POSSIBLES POUR LE SECTEUR PRIVÉ	20
	Résumé des problèmes	20
	Portée du document	22
	Politiques possibles	24
	Résumé	32

SYNOPSIS

Les progrès de la technologie des ordinateurs et des télécommunications ont soulevé des questions nouvelles sur la protection des renseignements personnels - c'est-à-dire le droit qu'ont les particuliers de savoir quelles informations sont recueillies à leur sujet et la façon dont elles sont communiquées à des tiers. Ce document de travail passe en revue un certain nombre de graves problèmes que risque de poser l'impact de l'évolution technologique sur la protection de la vie privée et examine divers moyens de les résoudre.

Les problèmes présentés portent sur la protection des données, la qualité des données, les limites de la divulgation, la défense de la sécurité, les coûts et l'accès individuel aux fichiers de renseignements personnels dans les banques de données informatisées. De récents sondages de l'attitude du public semblent indiquer que les particuliers sont très préoccupés par les effets de l'ordinateur sur leur vie privée et par les institutions qui recueillent trop de renseignements personnels à leur sujet.

Le secteur public a commencé à aborder ces problèmes par le biais de divers textes de loi qui définissent, pour les banques de renseignements des ministères et organismes gouvernementaux, les pratiques loyales en matière d'information et prévoient comment les appliquer. On peut citer, à titre d'exemple, la Loi fédérale sur la protection des renseignements personnels et le Bill 65 du Québec, assortis l'un et l'autre de bureaux mis en place pour veiller au respect des normes établies dans ce domaine et étudier les plaintes individuelles pour pratiques déloyales en matière d'information.

En Ontario, un projet de loi est à l'étude. Il s'agit du Privacy and Access to Information Bill, qui vise à imposer aux banques de données du gouvernement provincial des pratiques loyales en matière d'information. La loi serait accompagnée d'un bureau chargé de la faire appliquer et d'un autre qui serait habilité à recevoir les plaintes des citoyens en la matière.

En Europe, la protection des données est à l'ordre du jour et des pays comme le Royaume-Uni, l'Allemagne de l'Ouest et la Suède ont des programmes législatifs qui prévoient l'enregistrement des fichiers de données et régissent les pratiques en matière d'information dans les secteurs public et privé.

Le secteur privé, conscient du problème, a mis au point des méthodes internes et, dans certains cas, des codes volontaires visant à protéger les renseignements personnels suivant certains principes courants dans la législation sur le sujet. Aux États-Unis, Warner-Amex Cable Communications Inc. a mis au point un code qui protège le caractère confidentiel des données recueillies sur ses clients.

L'Association canadienne de télédistribution est en train d'élaborer un code de protection visant une auto-réglementation similaire.

Dans le passé, ce sont les bureaux de crédit, assujettis dans la plupart des provinces à des lois sur la divulgation des données relatives au crédit, qui ont été les principaux manipulateurs de renseignements personnels dans le secteur privé. On enregistre cependant un accroissement des fichiers informatisés de renseignements personnels dans toutes sortes de secteurs, notamment les institutions financières, les services de télédistribution, les services vidéotex, les services informatiques, ainsi qu'une multitude d'autres secteurs commerciaux et non commerciaux. Le particulier n'a pas de garantie concrète contre l'ingérence dans ces fichiers.

Si elles veulent aborder le problème de la protection de la vie privée de façon uniforme, les diverses instances canadiennes vont se heurter à un certain nombre de questions légales. À qui appartiennent les données personnelles contenues dans les fichiers? Comment peuvent-elles être légalement protégées? Les lois en vigueur sur la protection des données personnelles doivent-elles être amendées en fonction de l'évolution technologique? Qui est responsable de la divulgation impropre ou non autorisée de renseignements personnels? Et puis, bien sûr, il faudra faire face à l'éternel problème du partage des compétences entre les gouvernements fédéral, provinciaux et territoriaux, si l'on veut harmoniser les règlements à mesure qu'ils sont édictés et éviter les conflits entre les lois.

On estime généralement que les droits individuels, y compris les droits à la protection de la vie privée, ne relèvent de la compétence législative exclusive ni du gouvernement fédéral ni des gouvernements provinciaux, mais sont plutôt déterminés par la Constitution canadienne, et plus particulièrement par les articles 91 et 92 de l'Acte de l'Amérique du Nord britannique. Bien qu'un certain nombre de gouvernements aient déjà des lois sur la question, il est important que ces initiatives se poursuivent et, peut-être, s'amplifient.

Ce document de travail analyse quatre méthodes de résolution des problèmes que pose, pour la vie privée des citoyens, l'accroissement de la manipulation informatisée des données personnelles dans le secteur privé. Au lieu de passer en revue la gamme entière des mesures possibles, il en privilégie trois qu'il estime correspondre à la situation canadienne.

Le gouvernement a joué un rôle important dans la promotion et l'adoption de la technologie de la microélectronique et des communications. Maintenant que la technologie est acceptée dans tous les secteurs de l'économie, il lui incombe d'accorder son soutien à l'établissement de normes de protection de la vie privée.

La première approche possible consisterait, pour le gouvernement, à encourager l'auto-réglementation dans les industries qui font une utilisation importante de données. Cela pourrait prendre la forme de codes volontaires sur le modèle de ceux qu'utilisent certaines compagnies dont on parlera plus loin. Les tentatives d'auto-réglementation les plus dignes d'intérêt contiennent également des dispositions sur les pratiques loyales en matière d'information dans les contrats avec les clients. Le gouvernement pourrait travailler, de concert avec une association représentative de chaque secteur industriel, à mettre au point un code de respect de la vie privée correspondant à ce secteur. Cela produirait une série de codes volontaires conçus en fonction des exigences de chaque secteur.

Deuxièmement, le gouvernement pourrait aussi édicter des lois qui définissent les pratiques loyales en matière d'information et prévoient une pénalité en cas d'infraction. L'application de la loi pourrait être volontaire et ne concerner que les établissements qui choisissent de s'y conformer, ou obligatoire pour tous les secteurs qui font un usage important de données.

Une troisième méthode consisterait à établir un système d'enregistrement et de réglementation auquel seraient assujettis les utilisateurs de données. Ce système pourrait définir les principes majeurs de manipulation de l'information; instituer un registraire ou un commisariat pour administrer le système d'enregistrement et veiller à ce que les principes soient respectés; et établir le droit des particuliers touchant l'accès, la correction et la non-divulgation des données personnelles. On trouve des modèles de systèmes d'enregistrement dans la loi sur la protection des données (Data Protection Bill) du Royaume-Uni et dans les organes mis en place par les provinces canadiennes pour réglementer les renseignements personnels en matière de crédit.

Enfin, la combinaison de ces trois façons de procéder fournirait d'autres possibilités dont une qui mérite l'attention, à savoir une combinaison des systèmes d'auto-réglementation et d'enregistrement décrits ci-dessus. Aux fins de ce document, on a donné à cette méthode le nom d'"enregistrement volontaire". Les associations professionnelles pourraient élaborer des codes correspondant à leur secteur, veiller à ce que leurs membres s'y conforment et se faire les médiateurs des plaintes des particuliers. Ceci pourrait se faire en consultation avec un commissariat public à la protection de la vie privée qui tiendrait également un registre de toutes les associations et compagnies participantes.

PARTIE I : COMPRENDRE LES PROBLÈMES

Introduction

Il y a longtemps que le droit de l'individu à la protection de ses données personnelles et de sa vie privée - c'est-à-dire le pouvoir qu'il a de déterminer en grande mesure quels renseignements sont recueillis à son sujet et de quelle manière ils peuvent être utilisés par des tiers - constitue un aspect légitime d'une société libre. Or, bien que l'importance du respect de la vie privée soit généralement reconnue, son application dépendait en grande partie de l'impossibilité technologique où l'on se trouvait de procéder à une surveillance étendue et de tenir des dossiers détaillés sur un grand nombre d'individus. Cette barrière technologique n'existe plus. Il faut donc envisager d'établir des normes, si l'on veut que les données personnelles soient protégées dans le cadre du progrès technologique.

Pour prendre de telles mesures de sécurité, il est essentiel de s'accorder sur la définition de ce qu'on appellera des pratiques loyales en matière d'information. Ces pratiques fixeraient des limites générales à la façon dont les renseignements personnels sont recueillis, conservés et utilisés. Elles chercheraient aussi à équilibrer le droit de l'individu à la protection de sa vie privée avec les valeurs sociales et économiques également importantes d'ouverture et d'efficacité. Aux fins de ce document, on entendra par données personnelles les fichiers de renseignements sur une personne dans lesquels elle est identifiée par son nom ou facilement identifiable par d'autres moyens.

Le but de ce document de travail est de sensibiliser le lecteur aux problèmes majeurs que soulève l'impact possible de l'évolution technologique sur le droit des personnes à la protection de leur vie privée et de discuter des solutions possibles à leur apporter.

Les dernières innovations technologiques en matière d'ordinateurs et de télécommunications permettent de traiter et de relier des informations conservées dans diverses banques de données facilement, rapidement, et à bas prix. Au cours des vingt-cinq dernières années, la tenue des dossiers dans le secteur public et le secteur privé est passé de l'âge de la paperasse lente et encombrante, où les renseignements sont enregistrés à la main, au système de fichiers éclairs efficaces et lisibles par une machine. Cette évolution a eu un certain nombre de conséquences notables sur la vie privée des individus.

Tout d'abord, l'extraction de dossiers lisibles par une machine se fait plus rapidement et la mise à jour est plus facile et plus anonyme. Ce qui était autrefois un ensemble de documents dont la date était clairement apparente est devenu écran d'ordinateur. De plus, les dossiers informatisés sont facilement accessibles en des lieux éloignés de l'organisme. Ce qui est encore plus important, cependant, c'est qu'on peut facilement fusionner les dossiers informatisés, ce qui permet d'assembler dans un seul fichier un certain nombre de pièces traitant du même sujet ou de la même personne. Cela peut se faire au sein de l'organisme qui a recueilli les données, mais ces dernières peuvent également être transmises sans difficulté à un autre utilisateur d'informations et combinées avec d'autres dossiers en provenance d'autres sources, à des fins non prévues par les personnes touchées par le processus initial de collecte de l'information. Ceci est plus facile à accomplir si l'on a un numéro d'identification, mais le manque de numéro n'est pas un obstacle suffisant pour empêcher ce type de compilation. En outre, le réseau de télécommunications entre les détenteurs des dossiers permet de partager les fichiers constitués par un organisme à une fin bien précise avec d'autres utilisateurs qui poursuivent des fins bien différentes. On donne à ce processus le nom de raccordement des données.

L'impact possible, sur la protection de la vie privée, de la facilité avec laquelle les dossiers sont extraits, partagés et fusionnés se trouve multiplié par le nombre et la diversité des sources de renseignements informatisés sur les individus. Matériellement, les ordinateurs sont passés en vingt ans de l'état de machine de la taille d'une pièce à celui d'appareil facile à poser sur un bureau. Les coûts de l'équipement et du traitement ont baissé à la même allure. Pour se servir des anciens ordinateurs, il fallait avoir une formation poussée; les machines actuelles, qualifiées d'aimables pour l'usager, peuvent être utilisées avec un minimum de formation et de connaissances spécialisées.

Alors qu'autrefois, seules les institutions importantes, comme les gouvernements, disposaient des ressources nécessaires pour utiliser l'ordinateur de façon efficace, la tenue de dossiers informatisés est maintenant la norme dans presque tous les secteurs de l'activité humaine. Autrefois, le recensement national était l'unique compilation de renseignements divers sur les citoyens. Il est maintenant possible de rassembler des données encore plus diverses sur les individus, en partageant les informations entre les détenteurs de dossiers. Au gouvernement, le dossier de chaque personne comprend, entre autres, des renseignements sur l'état-civil, l'impôt, le casier judiciaire, la santé, la conduite automobile, les dossiers militaires et les dossiers scolaires.

Dans le secteur privé, les renseignements sur les individus qui figurent dans les dossiers informatisés sont encore plus variés. Parmi les plus connus, citons le dossier de solvabilité. Le public se préoccupe cependant de la constitution d'autres dossiers informatisés, notamment dans les secteurs des assurances, de la banque et des télécommunications. Il y a en outre beaucoup d'utilisateurs de données encore inconnus du public comme les détaillants qui ont un système de cartes de crédits ou les services d'achat par télévision, les magazines qui gardent les listes d'abonnement, les organismes de bienfaisance, commerciaux,

professionnels ou communautaires et autres prestateurs de services. Maintenant que la télédistribution entre dans une phase d'échange où il va être possible de se servir de la télévision pour procéder à ses opérations bancaires, faire ses achats, effectuer des sondages instantanés et commander les émissions de télévision sur la base du coût unitaire, le secteur privé va accumuler des quantités encore plus importantes de renseignements sur les individus.

Cette collection toujours grandissante de données personnelles est un élément quasi inévitable de la vie en ce dernier quart du vingtième siècle. Comme concluait, en 1977, une commission d'étude sur la protection de la vie privée aux États-Unis :

> Il est maintenant courant de demander à un particulier de donner des renseignements sur lui-même qui seront utilisés par des étrangers invisibles, lesquels prendront des décisions à son sujet qui influeront sur sa vie quotidienne. De plus, comme la majorité des services offerts par les organismes sont, ou du moins sont considérés comme des nécessités, le particulier n'a guère le choix et doit se soumettre à toutes les exigences des organismes qui lui posent des questions.

Pratiques loyales en matière d'information

Cette menace pour la protection de la vie privée a suscité un certain nombre de tentatives visant à fixer les limites appropriées et à protéger le caractère confidentiel des renseignements personnels conservés dans les systèmes informatisés. Les principes généraux énoncés dans la convention du Conseil de l'Europe sur la protection des individus en matière de traitement automatique des données personnelles sont un bon exemple des efforts tentés par les gouvernements pour établir des lignes directrices qui reconnaissent les avantages de la tenue de dossiers informatisés tout en respectant la valeur que les particuliers accordent à leur vie privée.

Ces lignes directrices sont basées sur les principes suivants :

i) Les renseignements personnels doivent être recueillis et traités de façon loyale et légitime.

ii) Les renseignements personnels doivent être conservés à une fin ou à des fins spécifiées et légitimes.

iii) Les renseignements personnels ne doivent pas être utilisés ni divulgués d'une manière incompatible avec lesdites fins.

iv) Les renseignements personnels doivent être adéquats, pertinents et d'une portée qui ne dépasse pas les fins spécifiées.

v) Les renseignements personnels doivent être exacts et, le cas échéant, remis à jour.

vi) Les renseignements personnels ne doivent pas être conservés sous une forme où figure le nom de la personne plus longtemps que nécessaire pour les fins spécifiées.

vii) Le sujet concerné par les renseignements doit avoir accès aux données qui existent sur son compte et être habilité à les corriger ou à les radier si les dispositions légales régissant lesdites données n'ont pas été respectées.

viii) Des mesures de sécurité appropriées doivent être prises contre l'accès sans autorisation, l'altération ou la dissémination, la perte accidentelle ou non autorisée des données.

Ces directives reconnaissent qu'il est nécessaire, pour l'individu, que les renseignements recueillis à son sujet le soient avec son consentement; que ce consentement soit basé sur une pleine et précise compréhension des fins auxquelles les renseignements sont recueillis; qu'il n'en soit pas fait usage sans son consentement; qu'il puisse avoir accès au fichier pour s'assurer que les renseignements sont corrects;

qu'en cas de désaccord sur l'exactitude des renseignements, sa version des faits soit notée et que des tiers n'aient pas accès à son dossier sans qu'il le sache ou le permette, sauf si c'est exigé par la loi.

Même s'il y a accord général sur ces principes dans les deux secteurs public et privé, il existe un certain nombre d'obstacles à leur réalisation. L'un de ces obstacles est le principe voisin de la liberté de l'information. Si un individu a le contrôle absolu sur toutes ses données personnelles, ce droit peut constituer un obstacle important au droit qu'ont les autres de se renseigner sur les activités gouvernementales. Il faut de toute évidence trouver un moyen terme.

Le problème du vol des données informatiques constitue un autre obstacle. Il s'agit du cas où des données sont saisies ou extraites sans la permission du détenteur du fichier de renseignements. On a suggéré d'apporter des amendements au Code criminel qui établiraient des infractions spécifiques en la matière et permettraient de résoudre en partie le problème. Les détenteurs de banques de données devraient cependant continuer à prendre des précautions raisonnables, au sein de leur organisation, pour faire en sorte que soit respecté le caractère confidentiel des renseignements personnels, et que les employés qui les manipulent se conforment aux mesures de sécurité nécessaires.

Le problème du passage des données d'un territoire à l'autre constitue un troisième obstacle en puissance. Il s'agit des renseignements sur des particuliers qui sont extraits et traités dans un autre territoire où la protection de la vie privée n'est pas assurée comme il se doit par le secteur privé ou par la loi. Ici aussi, l'efficacité et la valeur de la liberté de l'information risquent d'entrer en conflit avec les normes sur la protection des données personnelles. Certains de ces problèmes dépassent la portée de la présente discussion, car ils relèvent du gouvernement fédéral.

Perceptions du public

Des sondages récents indiquent que l'inquiétude devant la menace que représente, pour la protection des renseignements personnels, l'utilisation grandissante des ordinateurs n'est pas l'unique apanage des professeurs, des futurologues et des technocrates. Des sondages effectués pour le compte du gouvernement de l'Ontario en 1980 et 1983[1] indiquent qu'une majorité considérable de citoyens de l'Ontario sont préoccupés par l'impact des ordinateurs sur leur vie privée. En outre, en 1983, environ la moitié d'entre eux estimaient qu'il incombe essentiellement au gouvernement de protéger le caractère confidentiel des renseignements personnels et financiers dans notre société. Trente-huit pour cent des citoyens pensaient que c'était au secteur privé de protéger leur vie privée. Le premier sondage, effectué en 1980, révélait en outre qu'une minorité considérable de citoyens estimaient que les institutions comme le gouvernement, les dispensateurs de crédit, les employeurs et les compagnies d'assurance demandent aux particuliers trop de renseignements personnels et financiers.

Dans le même ordre d'idée, un sondage Gallup[2] de 1981 sur les attitudes envers la microélectronique demandait à la population de classer par ordre d'importance treize problèmes associés aux ordinateurs et à la technologie de l'information. La protection de la vie privée et le respect du caractère confidentiel des renseignements personnels venaient loin en tête et étaient mentionnés par 63% des personnes interrogées. Le nombre de gens ayant un pouvoir de contrôle sur l'information, problème étroitement lié au premier, était mentionné par 45 pour cent des personnes interrogées, ce qui classait cette préoccupation en troisième position. C'étaient les personnes qui déclaraient

---

1. Voir Ontario Consumer Issues 1980 et Préoccupations du consommateur ontarien en 1983

2. A Gallup Survey of Electronic Technology, mars 1981, The Gallup Organisation, Inc.

avoir des connaissances en microélectronique et les titulaires d'emplois dans le secteur de la vente, du travail de bureau et de l'administration qui se montraient le plus préoccupées par la protection de la vie privée. On demandait également aux personnes interrogées de se projeter cinq ans en avant et de dire si elles pensaient que leur vie privée serait alors "envahie ou gravement perturbée" par l'une ou plusieurs de dix-sept organisations, personnes morales ou individus. Le niveau d'inquiétude était élevé. Cinquante pour cent ou plus des personnes morales suivantes risquaient, à leur avis, d'envahir leur vie privée : une agence d'évaluation de la solvabilité, un ordinateur ou une banque de données, une compagnie d'assurance, le gouvernement fédéral ou provincial, une banque, une personne qui pourrait s'ingérer dans leur courrier et une autre qui communiquerait avec elles par téléphone. Une fois de plus, ce sont les personnes qui déclaraient connaître la microélectronique qui étaient le plus susceptibles de prévoir une invasion de leur vie privée.

Un sondage effectué en novembre 1982 à London, Ontario, par le professeur Neil Vilmar de l'université Western Ontario[3], pour le compte du gouvernement de l'Ontario, a révélé des niveaux pareillement élevés d'inquiétude pour la vie privée devant le développement des services interactifs de télédistribution. Plus des deux-tiers des personnes interrogées pensaient que leur vie privée était moins protégée au Canada que dix ans plus tôt. Parmi les types d'informations considérées les plus délicates et nécessitant le plus de protection, on citait les comptes en banque, le contrôle des entrées et des sorties de chez soi (câblotransmission utilisée par certains systèmes de sécurité), les dossiers de crédit, le salaire personnel et les dossiers médicaux. Les résultats indiquaient que près de la moitié des personnes interrogées s'inquiétaient de l'usage que faisait le gouvernement des renseignements recueillis, mais un pourcentage encore plus élevé était préoccupé par le secteur privé. Soixante-douze pour cent de l'échantillon

---

3. Neil Vedmar, Privacy and Two-way Cable Television: A Study of Canadian Public Opinion, Université Western Ontario, 1983.

donnaient la faveur à une réglementation par le gouvernement, une majorité de cinquante-deux pour cent accordant un rôle en la matière aux deux gouvernements fédéral et provincial. L'étude révélait également que la plupart des gens estimaient que les organismes publics et privés demandent davantage de renseignements personnels que nécessaire.

Réponse du secteur privé

Comme l'indiquent les directives de l'Organisation pour la coopération et le développement économique,[4] l'auto-réglementation des industries et des compagnies qui font un usage important de renseignements personnels constitue un des principaux moyens de protéger efficacement la vie privée des citoyens. À cet égard, plusieurs compagnies ont relevé le défi de l'auto-réglementation en établissant des pratiques internes bien pensées correspondant à la définition courante des pratiques loyales en matière d'information établie, entre autres, par l'OCDE.

Bell Canada, par exemple, est une corporation importante qui manipule une quantité considérable d'informations personnelles nécessairement recueillies aux fins de facturation. Les politiques de la compagnie considèrent tous les renseignements de l'abonné à l'exception de son nom, de son adresse et de son numéro de téléphone, comme des informations privées conservées uniquement pour répondre aux besoins au sein de la compagnie. Les données personnelles ne peuvent pas être vendues et les employés de Bell sont informés que tout renseignement sur les abonnés, où qu'ils soient recueillis, sont strictement confidentiels. En fait, l'existence, le contenu ou la nature de toute communication de l'abonné ne doit pas être communiqué à un tiers sauf pour se conformer à une ordonnance légale. Dans le cas d'une telle ordonnance, Bell avisera l'abonné, à moins qu'on ne le lui défende spécifiquement.

---

4. Organisation pour la coopération et le développement économique, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

La Banque de Montréal est un autre utilisateur de données personnelles qui a mis au point des pratiques spécifiques de protection des renseignements personnels et publié des informations à ce sujet. Les données recueillies et gardées en dossier constituent le minimum nécessaire pour dispenser le service requis. Au sein de la compagnie, l'accès à ce type de renseignement est étroitement contrôlé et aucune information n'est généralement fournie à un tiers sans le consentement du client, sauf pour se conformer à la loi ou à une ordonnance du tribunal. Les demandes de carte de crédit, les prêts personnels et les hypothèques, cependant, comprennent une clause de consentement général ou de renonciation qui autorise la banque à divulguer des renseignements sur le client à des tiers dans certaines circonstances. La pratique qui consiste à faire signer des renonciations aux clients, courante dans les institutions financières, a été critiquée dans le passé au nom de la protection de la vie privée du client.

Le secteur de la télédistribution du Canada a chargé son association, l'Association canadienne de télédistribution, de mettre au point un code général de protection des renseignements personnels qui lui permettra de s'auto-réglementer. Un sous-comité de l'association, sur le modèle du code hautement respecté de l'institution américaine de câblodiffusion Warner Amex, est en train d'élaborer un code correspondant à la scène canadienne. On prévoit que ce code sera accepté et appliqué par les compagnies membres de l'association alors qu'elles mettent au point les services interactifs qu'elles vont offrir au public. L'établissement d'un code avant le développement des services présente un avantage majeur, car les systèmes peuvent être conçus à l'avance pour renforcer la sécurité informatique et les possibilités de protection des données.

Il n'en demeure pas moins que les compagnies pourvues d'un code de protection volontaire constituent l'exception plutôt que la règle. Il est donc clair que la vaste manipulation informatisée des renseignements personnels devra être assujettie à un système de normes quelconque pour veiller à ce que la vie privée des citoyens ne soit pas violée.

PARTIE II : LOIS RÉGISSANT LES BANQUES DE DONNÉES DU SECTEUR PUBLIC

Le nombre de lois visant, au Canada et à l'étranger, à répondre aux problèmes que posent l'accès à l'information et la protection des renseignements personnels va croissant. La plupart sont d'origine récente, ce qui est révélateur de leur rapport étroit avec le développement de la technologie de l'information et de la rapidité avec laquelle les innovations risquent de soulever de graves questions en matière de protection de la vie privée. Dans cette section seront passées en revue un certain nombre de solutions, dont certaines ne s'attachent qu'aux banques de données gouvernementales alors que d'autres visent également le secteur privé.

Canada

Au niveau canadien national, l'effort porte essentiellement sur l'élaboration de pratiques loyales en matière d'information dans les fichiers relevant de la compétence fédérale. La Loi sur la protection des renseignements personnels, adoptée en 1982 et proclamée en 1983, confère aux citoyens canadiens et aux résidents permanents le droit d'être informés, à certaines exceptions près, de l'existence de dossiers à leur sujet, d'examiner, de corriger et de remettre en question les renseignements qui s'y trouvent; de savoir quel usage a été fait du dossier; et d'être consultés avant qu'il en soit fait un autre usage. Une loi voisine, la Loi sur l'accès à l'information a été édictée pour maximaliser la compatibilité entre l'accès à l'information et la protection de la vie privée. La Loi sur la protection des renseignements personnels exige que soit publié un répertoire annuel des fichiers fédéraux de données personnelles et crée un Commissaire à la protection de la vie privée habilité à jouer le rôle du médiateur en cas de litige, à enquêter pour veiller à ce que la loi soit observée par les détenteurs de fichiers et à exercer son droit de recours en révision devant la Cour des décisions gouvernementales touchant lesdits renseignements.

Provinces

La Nouvelle-Écosse et le Nouveau-Brunswick ont édicté l'une et l'autre des lois sur la liberté de l'information vers la fin des années 1970. La loi de Nouvelle-Écosse énumère les types de documents auxquels on peut avoir accès plutôt que d'établir un principe général d'accès, alors que le Nouveau-Brunswick établit des principes généraux, avec possibilité d'appel à un ombdusman et inspection à huit-clos des documents contestés par les tribunaux.

La Nouvelle-Écosse a adopté des lois sur la liberté de l'information et la protection des renseignements personnels en 1981. La première loi dresse la liste des ministères, conseils, organismes et commissions visés et l'autre fait de la violation, par une personne, de la vie privée d'un individu un tort exécutoire sans preuve de dommage.

Le Québec traite en même temps la liberté d'information et la protection des renseignements personnels dans une loi adoptée en 1982 et destinée, comme la loi fédérale, à protéger les données personnelles contenues dans les fichiers gouvernementaux, tout en permettant l'accès aux documents des organes publics. Ces organes comprennent non seulement le gouvernement provincial et tous ses ministères et organismes, mais aussi les municipalités (gouvernement et institutions gouvernementales aux paliers du comté, de la région et de la ville), les établissements d'enseignement et les institutions de santé et de services sociaux. La loi exige que la commission d'accès à l'information compile aux fins de circulation un répertoire des dossiers tenus par les organes publics et que les demandes d'information reçoivent gratuitement une réponse dans les 20 jours qui suivent leur réception. La commission a des pouvoirs divers de supervision, d'enquête et de décision.

Dans le passé, l'Ontario a sérieusement étudié les questions d'accès à l'information et de protection des renseignements personnels. Il en est résulté un projet de loi, le Privacy and Access to Information Bill, visant à définir les pratiques loyales en matière d'information et à les rendre obligatoires dans les fichiers de renseignements personnels du gouvernement. Le projet prévoit d'établir un bureau de la protection des données qui aurait le pouvoir d'élaborer et de faire appliquer des normes auxquelles seraient assujettis les systèmes de données personnelles. Ces normes exigeraient, entre autres, que soit limitée la collecte de données au minimum essentiel à l'opération d'un programme; que les renseignements personnels soient normalement recueillis directement auprès du sujet et que la raison de la collecte lui en soit communiquée; et, de manière générale, que les renseignements recueillis ne soient pas divulgués sans le consentement de l'individu. Feraient exception à la règle relative à la divulgation les cas où celle-ci ne représenterait pas une ingérence injustifiée dans la vie privée de l'individu et où elle serait nécessaire à l'administration de programmes gouvernementaux autorisés ou au meilleur intérêt de l'individu ou de la société. Les particuliers auraient le droit d'accéder à leur dossier et d'y apporter des corrections, le détenteur des données étant tenu de notifier les utilisateurs passés du dossier de tout amendement à celui-ci. Les particuliers auraient également le droit de porter plainte devant le bureau séparé d'un commissaire.

En 1968, la Colombie-Britannique a adopté une loi sur la protection des renseignements personnels, ce qui en a fait le premier gouvernement du Commonwealth à établir un recours indépendant en cas d'ingérence déraisonnable et injustifiée dans la vie privée d'un individu. Cette loi a été suivie par des textes semblables au Manitoba et en Saskatchewan. Cependant, aucune de ces lois ne traite expressément de l'utlisation inappropriée ou non autorisée des renseignements personnels donnés volontairement à une autre personne ou à une autre institution et intégrés dans un fichier informatisé.

De plus, le coût du recours aux tribunaux risque de faire hésiter l'individu à se prévaloir de ses droits, les coûts du procès dépassant souvent ses avantages possibles.

États-Unis

La loi américaine sur la protection des renseignements personnels date de 1974 et vise les données personnelles contenues dans les fichiers gouvernementaux. Il s'agit essentiellement d'un texte à fonctions domestiques qui établit des normes pour l'administration des fichiers de données. À cet égard, il exige du gouvernement qu'il fasse rapport sur l'existence de fichiers de renseignements personnels, qu'il veille à la qualité des données qui s'y trouvent, qu'il permette aux sujets de ces fichiers d'y avoir accès, d'utiliser uniquement les données aux fins pour lesquelles elles ont été recueillies et de tenir un dossier de la divulgation des informations aux personnes concernées. Les réponses aux questions ne sont pas limitées dans le temps et la loi s'applique d'elle-même dans la mesure où la personne lésée saisit les tribunaux de sa plainte plutôt que de s'adresser à une instance séparée. Les États-Unis ont également une loi sur la liberté de l'information qui confère des droits d'accès relativement plus étendus que la loi sur la protection des renseignements personnels.

Royaume-Uni

Le parlement britannique est en train d'élaborer une loi sur la protection des données qui vise les fichiers informatisés de renseignements personnels des deux secteurs public et privé. Ce projet établit un registraire et un tribunal de protection des données; exige l'enregistrement (à certaines exceptions près) des fichiers de renseignements personnels publics et privés; prohibe la divulgation non autorisée des informations; permet aux particuliers d'avoir accès aux données détenues dans les fichiers enregistrés et les habilite à amender les dossiers et à chercher compensation auprès des tribunaux en cas de préjudice.

Le registraire est habilité à annuler l'enregistrement des fichiers de renseignements personnels qui contreviennent aux principes de protection desdites données et peut empêcher le transfert de renseignements du Royaume-Uni dans un pays qui ne respecte pas les normes minimales en la matière. Cette loi permettra au Royaume-Uni d'adhérer à la convention du Conseil de l'Europe sur la protection des données.

<u>République fédérale de l'Allemagne occidentale</u>

La République fédérale allemande n'a pas de loi générale sur l'accès à l'information mais un réseau hautement développé de dispositions visant à protéger les renseignements personnels et à sauvegarder la vie privée des individus. Il s'agit d'une part de la loi fédérale sur la protection des renseignements personnels et des lois des états sur le même sujet qui intègrent les principes de protection des données du Conseil de l'Europe. La loi fédérale vise également les fichiers de renseignements personnels du secteur public fédéral et du secteur privé à l'échelle du pays, alors que les lois des états régissent les pratiques en la matière de leurs gouvernements respectifs. C'est aux directeurs des institutions gouvernementales qui créent et utilisent les fichiers de renseignements personnels qu'il incombe en priorité de veiller au respect des lois. De même, les lois du palier fédéral et des états prévoient la mise en place du bureau d'un commissaire à la protection des données personnelles, chargé de superviser et de conseiller les organismes qui manipulent des fichiers de renseignements personnels et de faire rapport au parlement une fois par an. Le succès de ce système de protection ne vient pas des pouvoirs de coercition de la commission à la protection des renseignements personnels mais du degré élevé de sensibilisation du public et du gouvernement aux pratiques appropriées en matière de manipulation des données.

Suède

La Suède a été le premier pays du monde à promulguer des lois sur l'accès à l'information et la protection des renseignements personnels. L'accès aux renseignements détenus par le gouvernement est réglementé par la loi sur la liberté de la presse et la loi sur la protection des renseignements personnels qui, ensemble, permettent l'accès général dans le cadre de certaines exceptions spécifiques et limitées. Le caractère confidentiel de l'information est garanti par plusieurs textes législatifs dont le plus important est la loi sur les données personnelles de 1973. Cette loi a créé une commission d'inspection des renseignements personnels qui réglemente la collecte et l'utilisation des fichiers informatisés dans les deux secteurs public et privé. La fonction majeure de la commission est donc de délivrer des permis à tous les fichiers de renseignements détenus par le gouvernement ou par les utilisateurs du secteur privé et d'édicter des règlements qui régissent leur usage. On peut appeler des décisions de la commission au ministre de la justice et au cabinet, mais le nombre de ces appels n'a jamais été élevé. De façon générale, le système qui régit l'utilisation des renseignements fait passer la protection de la vie privée avant les considérations d'économie et d'efficacité.

Conseil de l'Europe

Le Conseil de l'Europe a préparé une convention pour la protection des individus relativement au traitement automatisé des renseignements personnels, qui vise à assurer le respect du droit de l'individu à la protection de sa vie privée. Elle requiert des états signataires qu'ils intègrent dans leurs lois nationales les principes de base définis dans la convention à savoir : emploi de pratiques loyales en matière d'information; limites imposées à l'utilisation et au contenu des fichiers en fonction des fins auxquelles les données sont recueillies; exactitude; identification minimale des individus; limites imposées aux types de données à traiter; mesures de sécurité appropriées;

et procédures pour permettre aux sujets des dossiers d'identifier ces derniers, de les examiner et de les corriger. La convention confirme également le droit qu'ont les états signataires de refuser que des renseignements personnels soient envoyés dans des pays n'offrant pas une protection similaire.

Organisation pour la coopération et le développement économique. (OCDE)

Le Conseil de l'OCDE a établi des directives régissant la protection des renseignements personnels qui contituent les normes minimales que doivent respecter ses membres. Sur le modèle de la convention du Conseil de l'Europe, l'OCDE souscrit aux principes suivants: limite de la collecte, qualité des données, spécification des fins auxquelles elles sont utilisées, limitation de l'utilisation, mesures de sécurité, ouverture, participation individuelle, responsabilité. Tout en énonçant spécifiquement que la protection des renseignements personnels ne doit pas servir d'alibi pour limiter leur passage au-delà des frontières, l'OCDE convient que les pays membres doivent empêcher toute exportation de données qui circonvient les lois nationales sur la protection des renseignements personnels ou dans des pays ne respectant pas en substance les principes auxquels il souscrit. Les pays membres sont invités en particulier à : adopter des lois nationales appropriées; encourager et soutenir l'auto-réglementation; conférer aux individus un moyen raisonnable d'exercer leurs droits; prévoir des sanctions adéquates; et veiller à ce que les sujets des dossiers ne fassent pas l'objet de discriminations injustes.

Résumé

On a pu voir dans ce qui précède que les diverses lois édictées par différentes autorités couvrent un très vaste territoire. La plupart souscrivent à un ensemble similaire de pratiques et de principes loyaux en matière d'information.

Bien qu'il y ait divergence sur des points de détail, lorsqu'il s'agit par exemple de décider si les renseignements recueillis doivent être "pertinents" et recueillis "directement", la plupart des lois confèrent à l'individu le droit d'accès et de correction et exervent un certain contrôle sur la transmission des renseignements personnels à un tiers. Au-delà de ces similarités de base, cependant, ces lois varient énormément au niveau de leur portée et de leur application.

Aux fins de ce document, il paraît utile de prendre acte de trois des modèles discutés ci-dessus. À une extrémité du spectre, la loi américaine sur la protection des renseignements personnels est un exemple de loi qui définit certains droits individuels mais n'établit pas d'organe séparé pour en assurer le respect. Aux termes de cette loi, c'est à l'individu de saisir les tribunaux de ses griefs.

Un second modèle, illustré par la Loi canadienne sur la protection des renseignements personnels, établit un organe d'exécution nanti de pouvoirs d'enquête et de contrôle. Les particuliers lésés peuvent porter plainte auprès du Commissaire à la protection de la vie privée qui peut également prendre l'initiative d'une plainte et exercer le recours en révision pour refus de communication. La nouvelle loi du Québec est assez semblable, bien que son champ d'application soit plus vaste et couvre notamment les municipalités, les conseils scolaires, les universités et les organismes de santé et de service social, en plus des ministères du gouvernement. La loi du Québec confère à sa commission le pouvoir considérable de surveiller les pratiques en matière d'information, d'instruire les plaintes, de faire enquête et de rendre des ordonnances de force exécutoire.

Le troisième modèle, à l'autre extrémité du spectre, est illustré par le système d'enregistrement du Royaume-Uni décrit ci-dessus. Sous certains aspects, ce système de réglementation est plus fort que les deux modèles

précédents, car il requiert l'enregistrement formel des fichiers de renseignements personnels et confère au registraire des pouvoirs substantiels d'enquête et d'application, notamment le pouvoir de refuser d'enregistrer un fichier si son utilisateur ne se conforme pas aux dispositions de la loi. Les systèmes d'enregistrement suédois et allemand vont encore plus loin et constituent deux modèles supplémentaires.

PARTIE III : SOLUTIONS POSSIBLES POUR LE SECTEUR PRIVÉ

Résumé des problèmes

La première partie de ce document exposait la menace que constitue pour la vie privée des citoyens la manipulation automatisée des renseignements personnels. Il s'en dégage un certain nombre de notions concurrentes. La plupart des gens conviennent qu'il faut pondérer les avantages de l'ordinateur en matière d'efficacité et de vitesse par l'évaluation de ce qu'il en coûte au niveau de la protection de la vie privée des individus. En termes d'économie, les institutions commerciales sont donc soumises à des pressions conflictuelles qui visent d'une part à profiter de toutes les économies que permet de réaliser la technologie nouvelle et, d'autre part, à garantir à l'individu la protection des renseignements personnels le concernant.

Bien qu'il soit difficile de généraliser, il appert que le coût de la protection minimale de la vie privée n'est pas très élevé par rapport aux économies que la nouvelle technologie permet de réaliser au niveau de l'efficacité. De plus, ces coûts de "protection" sont souvent minimisés si l'on fixe des normes ou des procédures avant d'introduire les nouveaux systèmes.

Les problèmes exposés dans la partie I peuvent se résumer comme suit :

1) Collecte des données : Les renseignements personnels recueillis par les utilisateurs de données[5] doivent-ils se limiter à ce qui relève spécifiquement

---

5. Les définitions suivantes sont utilisées dans ce document : Utilisateur de données : Institution qui recueille et manipule des fichiers de renseignements personnels sur les particuliers. Sujet des données : Individu qui fait l'objet de la collecte de données.

de l'objectif de l'utilisateur et à ce qui a fait l'objet du consentement éclairé du sujet? Faudrait-il exiger en outre que les renseignements personnels soient recueillis directement auprès du sujet auquel ils se rapportent? Les principales déclarations de principe sur le problème de l'obtention des données sont généralement assorties d'une clause à l'effet que ces dernières doivent être recueillies en toute justice et légitimité, à une fin elle-même légitime. Ce document part du principe que la légitimité ne constitue pas un problème et s'attache à la pertinence de la collecte des données et au consentement éclairé du sujet.

2) Qualité des données : Les renseignements personnels recueillis par les utilisateurs de données doivent-ils être assujettis à des exigences d'exactitude, de complétude et de remise à jour?

3) Limitations de la divulgation : La communication, par les utilisateurs de données, de renseignements personnels à des tiers doit-elle se limiter aux renseignements requis pour atteindre l'objectif spécifié par l'utilisateur? Feraient exception à cette règle les cas où il y a consentement du sujet ou ceux qui tombent sous le coup de la loi.

4) Mesures de sécurité : Les utilisateurs de données doivent-ils obligatoirement veiller à la sécurité physique des fichiers de renseignements personnels?

5) Accès individuel : Les particuliers doivent-ils avoir le droit de vérifier l'existence de dossiers personnels à leur sujet, d'inspecter et de recevoir une copie des renseignements qui y sont contenus et de demander que soient modifiées les données erronées ou incomplètes?

6) Coûts : Si l'on donne aux citoyens le droit d'accès, de modification et de non-divulgation, les coûts d'application de ces droits ne doivent pas être rédhibitoires. Les règlements qui confèrent à des organismes d'application de la loi le pouvoir quasi judiciaire de régler les griefs constituent un moyen de conférer aux particuliers des droits susceptibles d'être respectés.

Cette section analyse un certan nombre de solutions aux problèmes qui se posent dans le secteur privé et passe en revue les points forts et les faiblesses de chacune. On part du principe que la protection des renseignements personnels est une exigence légitime et que les principes énoncés par la convention du Conseil de l'Europe sur la protection des données (résumés en page 5) représentent une référence raisonnable pour l'évaluation des solutions proposées.

Portée du document

Ce document vise les deux secteurs, public et privé. Du point de vue du citoyen individuel, les deux secteurs représentent une menace pour la protection de la vie privée. Bien qu'en Amérique du Nord, les lois sur la protection des renseignements personnels n'aient visé jusqu'à présent que le secteur public, des pays comme le Royaume-Uni[6], l'Allemagne de l'Ouest et la Suède ont des programmes législatifs qui couvrent les deux secteurs.

La question du choix se présente alors entre l'auto-réglementation et la réglementation gouvernementale. On examinera ci-dessous les avantages et les inconvénients de l'auto-réglementation comme moyen de garantir que le secteur privé adopte des pratiques loyales en matière d'information.

---

6. Au moment de la rédaction de ce rapport, le projet de loi britannique avait été accepté en seconde lecture

Il est une autre question que les gouvernements doivent régler. Il faut en effet décider si les programmes de réglementation doivent couvrir seulement les fichiers informatisés de renseignements personnels ou s'appliquer à tous les dossiers, aussi bien manuels qu'informatisés. Le principe majeur du livre blanc[7] du Royaume-Uni sur la protection des données est que l'automatisation présente de nouvelles menaces pour la protection de la vie privée, à cause de la vitesse et de la facilité avec laquelle les renseignements personnels peuvent maintenant être communiqués à un coût relativement peu élevé. Cela sous-entend que l'argent et les efforts que demande le transfert manuel des renseignements freinent d'eux-mêmes la divulgation non autorisée.

En revanche, les lois sur la protection des données qui visent les dossiers du secteur public d'Amérique du Nord ne distinguent pas entre fichiers informatisés et dossiers manuels. Ces lois confèrent à l'individu certains droits en matière de protection des renseignements personnels dans les deux types de dossier. On peut se rendre compte de l'importance des dossiers manuels dans le cas, par exemple, des archives médicales.

Il faut également se demander si tous les fichiers de renseignements personnels devraient être couverts par la réglementation imposée ou l'auto-réglementation, ou seulement ceux dont la taille dépasse un certain seuil. Certains insistent sur le fait que seuls les utilisateurs de données d'une certaine importance devraient être assujettis à la réglementation, les coûts d'application constituant un fardeau plus élevé pour les organismes moins importants. L'exemption des banques de données plus petites, cependant, laisserait ces renseignements sans protection et affaiblirait par là même les droits individuels.

---

7. Data Protection: The Government' Proposals for Legislation, ministère de l'Intérieur, Royaume-Uni, avril 1982.

Politiques possibles

Cette section passe en revue quatre solutions possibles : un code volontaire de protection des renseignements personnels, un code aux termes d'une loi, un système d'enregistrement et de réglementation, et une méthode combinant les éléments des trois premières propositions. Cette liste n'a pas la prétention d'être exhausive mais vise à encourager la discussion des diverses solutions qui semblent raisonnablement correspondre à la situation canadienne.

1) Code volontaire de protection des renseignements personnels : Une fois admise la légitimité de la protection des données personnelles, les gouvernements pourraient inciter les industries spécifiques (par le biais de leurs associations) et les corporations qui font un usage important de données à élaborer des codes volontaires qui intégreraient les principes importants qui figurent habituellement dans les lois sur la protection de la vie privée. Des compagnies comme Warner-Amex aux États-Unis et IBM en Europe ont déjà mis au point des directives pour la protection des renseignements personnels contenus dans leurs fichiers. Au Canada, l'Association canadienne de télédistribution est en train d'élaborer un code.

En 1981, Warner-Amex Cable Communications Inc. a mis au point un code visant à protéger le caractère confidentiel des renseignements personnels que la compagnie compile sur les abonnés au service de télédistribution. Dans ce code, la compagnie s'engage à garantir la sécurité matérielle et le caractère confidentiel des renseignements sur les abonnés et à informer ces derniers de toutes les fonctions des services de télédistribution qui donnent lieu à une collecte de renseignements. Un accord passé avec chaque abonné énonce les conditions d'utilisation des renseignements et prévoit que nulle autre donnée individuelle ne sera recueillie sans le consentement de l'individu. Le code donne également à l'abonné le droit d'examiner son dossier et d'exiger la correction des données erronées.

Le code est en train de s'intégrer aux contrats et aux accords de franchise passés avec les abonnés, ce qui le rend auto-applicable et confère à l'abonné certains droits. En théorie, tout individu qui estime que son droit à la protection de sa vie privée a été violé peut intenter des poursuites pour bris de contrat.

Commentaires : On peut résumer de la manière suivante les avantages et les inconvénients de la méthode du code volontaire en réponse aux problèmes posés par la protection des renseignements personnels;

- Elle ne garantit pas que la majorité des institutions qui font un usage important de données adopteront volontairement un code.
- Elle ne propose pas de système formel d'application ni de respect des codes (à l'exception du pouvoir limité qu'a le particulier d'intenter des poursuites pour bris de contrat, dans le cas où le code est assorti d'un accord écrit entre l'utilisateur et le sujet des données).
- Les coûts et difficultés qu'elle entraîne pour les utilisateurs de données sont minimaux.
- Elle présente une flexibilité maximale, les codes pouvant s'adapter à l'évolution de la technologie et des exigences du public.
- Elle ne garantit pas de droits substantiels à l'individu en cas de litige sur l'accès, la correction ou la divulgation.
- L'adoption de divers codes volontaires par divers secteurs et compagnies industriels risque d'aboutir à un manque d'uniformité de la protection offerte aux individus.

2) Code imposé par la loi : À mi-chemin entre les codes volontaires et les règlements gouvernementaux plus traditionnels, une autre méthode propose d'édicter une loi qui définirait les pratiques loyales en matière d'information et prévoirait des pénalités pour toute

infraction à ces pratiques. Lesdites pratiques pourraient couvrir la collecte et la qualité des données, les limites à la divulgation, les mesures de sécurité et l'accès individuel tels que définis ci-dessus. Cette loi permettrait d'intenter une action délictuelle au civil et constituerait essentiellement une médhode d'auto-réglementation du problème sans le secours d'un organe d'exécution.

Certains auteurs ont suggéré que les exigences du public en matière de protection de la vie privée viennent de ce que les parlements et tribunaux n'ont pas déjà élaboré ce type de loi[8]. On convient généralement que la common law en vigueur dans les pays du Commonwealth n'offre pas en soi de protection de la vie privée.

Les lois sur la protection des renseignements personnels édictées par la Colombie-Britannique, la Saskatchewan et le Manitoba n'ont pas souvent été utilisées et, de l'avis général, ne proposent pas de remède susbstantiel au type de problème que pose à l'individu la manipulation automatisée des données personnelles.

Une loi prévoyant un code de protection des renseignements personnels pourrait prendre l'une des deux formes suivantes :

a) Une loi qui permettrait l'acceptation volontaire du code. Les règlements afférents à ce type de loi enregistreraient les industries ou compagnies qui souhaitent se conformer au code. Les participants volontaires seraient ainsi identifiés dans leur secteur comme des compagnies conscientes des problèmes de protection de la vie privée.
b) On peut aussi songer à une loi qui exigerait le respect du code. Elle s'appliquerait à tous les utilisateurs de données ou seulement aux fichiers de renseignements personnels dont l'importance dépasse un certain seuil.

---

8. Voir par exemple, Roger Noll, "Regulation and Computer Services", dans M. Dertouzos et J. Moses, The Computer Age: A Twenty-Year Review, (Cambridge: MIT Press, 1980) et Murray Rankin, Privacy and Technology: A Canadian Perspective (Canadian Institute for Legal Studies, Cambridge University, 1983).

Commentaires: On trouvera ci-dessous un résumé des points forts et des faiblesses de cette méthode:

- Elle ne garantit pas qu'une majorité des utilisateurs de données se conformera volontairement au code. Seule la version obligatoire d'un tel statut garantit la participation d'une majorité des utilisateurs de données.
- Le remède proposé aux particuliers est coûteux et compliqué. Il ne serait sans doute pas souvent utilisé, les coûts pour le particulier dépassant presque toujours les avantages possibles du remède. Il s'ensuit que cette approche ne confère pas de droits substantiels à l'individu relativement à l'accès, la correction, la divulgation des renseignements et la résolution des litiges.
- Les coûts et les complications pour les utilisateurs de données sont minimaux.
- La méthode offre un degré élevé de flexibilité, les pratiques loyales en matière d'information étant définies dans la loi en termes généraux qui ne gèneraient pas l'application de nouvelles techniques.
- Si le recours des particuliers au remède prévu reste limité, ce type de loi n'aura pas d'impact majeur sur les pratiques en matière d'information. La version obligatoire de ce type de loi, cependant, peut favoriser une certaines uniformité dans la collecte générale des données et les pratiques générales en matière de divulgation.

3) Enregistrement et réglementation : Une autre solution possible au problème serait que les gouvernements édictent des lois qui exigent l'enregistrement des fichiers de renseignements personnels, donnent aux individus des droits d'accès et de correction bien définis; réglementent la collecte de renseignements personnels et leur divulgation à des tiers; garantissent la sécurité des données; et établissent un registraire habilité à faire enquête et à faire appliquer la loi. L'exigence d'enregistrement pourrait s'appliquer aux institutions qui constituent des fichiers informatisés de renseignements personnels.

C'est là, fondamentalement, la méthode adoptée par le Royaume-Uni dans le projet de loi sur la protection des données (Date Protection Bill) présenté dans la deuxième partie de ce document. Ce texte institue un système d'enregistrement et d'application de la loi à l'intention des usagers de fichiers informatisés de renseignements personnels. Bien que le système d'enregistrement s'applique également au secteur public et au secteur privé, sa structure fondamentale peut servir de modèle utile aux fins de discussion.

Dans ce modèle, le registraire public des utilisateurs de données sensibilise les individus à l'existence des fichiers informatisés de renseignements personnels et aux objectifs qu'ils visent. L'utilisateur de données doit s'identifier, dire quels renseignements il utilise, d'où ils proviennent, à qui ils sont communiqués et à quelles fins ils sont utilisés. Le registraire a le pouvoir de faire enquête, d'inspecter les dossiers et d'exiger des modifications au système. Dans les cas extrêmes, il peut refuser l'enregistrement pour non-conformité aux termes des grands principes de protection des renseignements personnels prévus par la loi. Étant donné les pouvoirs étendus du registraire, ce type de loi institue un processus d'appel à un tribunal indépendant composé d'experts en droit et en informatique.

Le texte proposé par le Royaume-Uni donne également à l'individu le droit d'accès aux renseignements personnels; le droit à la compensation pour préjudice causé par l'utilisation de données erronées, la perte de données et la divulgation non autorisée ainsi que le droit de recours aux tribunaux pour demander la rectification ou la radiation des données incorrectes. C'est au particulier de saisir les tribunaux de sa plainte en cas de violation de ses droits individuels pour exiger le respect de la loi ou réclamer des dommages-intérêts.

D'autres dispositions du même texte permettent au gouvernement de restreindre le transfert de certaines catégories de renseignements dans des pays spécifiés où la protection des données ne fait pas l'objet d'une réglementation aussi stricte, d'autoriser l'établissement de règlements pour régir certaines catégories de données personnelles comme l'origine raciale, les appartenances politiques et les croyances religieuses; et d'exempter des dispositions de la loi les collectes de données effectuées aux fins de recherches, si les individus ne sont pas identifiables.

Les commentaires suivants ne s'attachent qu'aux caractéristiques générales d'un système d'enregistrement de ce type tel qu'il serait appliqué au secteur privé. Il ne s'agit pas d'une évaluation de l'ensemble du texte.

Commentaires : Les avantages et inconvénients de cette méthode peuvent se résumer comme suit :

- Elle prévoit aux termes de la loi la protection des renseignements personnels recueillis par les utilisateurs les plus importants et l'assortit d'un mécanisme chargé de faire observer ladite loi.
- Elle confère à l'individu des droits légaux d'accès et de correction ainsi que de protection contre la divulgation à des tiers. En cas de litige, cependant, la défense de ces droits peut s'avérer coûteuse pour l'individu qui doit s'adresser aux tribunaux.
- Elle impose de nouveaux règlements au secteur privé, c'est-à-dire des coûts supplémentaires aux utilisateurs.
- Elle permet une certaine souplesse car les principes de protection des données sont généraux tout comme les pouvoirs du registraire, ce qui leur permet de s'adapter à l'évolution de la technologie et des pratiques en matière d'information.
- Le système d'enregistrement et les pouvoirs d'exécution auraient un effet marqué sur les pratiques en matière d'information.

Les sytèmes d'enregistrement sont courants dans les lois sur la protection des renseignements personnels des autres pays européens. On a donné, dans la deuxième partie, une brève description des lois de l'Allemagne de l'Ouest et de la Suède, sans doute les deux exemples les plus dignes d'intérêt.

L'inconvénient majeur de ce modèle, du point de vue de l'individu, est ce qu'il lui en coûte de s'adresser au tribunal pour faire respecter ses droits. Un autre système d'enregistrement pourrait comporter, pour le citoyen, une possibilité d'appel à un registraire ou à un commissaire dont les ordonnances auraient force exécutoire pour l'utilisateur de données. Ceci résoudrait le problème du coût rédhibitoire pour le particulier.

De nombreuses provinces canadiennes ont édicté des lois qui réglementent la collete et la divulgation des renseignements personnels en matière de crédit. En Ontario, par exemple, la loi sur les renseignements concernant le consommateur enregistre les bureaux de crédit, réglemente la collecte, la conservation et la divulgation des renseignements en matière de crédit et confère à l'individu le droit d'accès à son dossier de crédit personnel. Le registraire est habilité à révoquer ou à refuser l'enregistrement dans certaines circonstances, auquel cas le candidat peut faire appel à un tribunal. Les modèles utilisés par les provinces pour réglementer les renseignements en matière de crédit pourraient fournir une orientation au système d'enregistrement envisagé pour les utilisateurs de fichiers de renseignements personnels.

4. <u>Enregistrement volontaire</u> : On pourrait envisager d'autres possibilités en combinant les trois approches ci-dessus. Une méthode digne d'intérêt consisterait à combiner les deux systèmes d'auto-réglementation et d'enregistrement. Les associations industrielles pourraient élaborer des codes de protection des renseignements personnels qui correspondent à leur secteur, veiller à ce que

leurs membres honorent lesdits codes et servir de médiateur en cas de plaintes de la part des citoyens. Ceci pourrait se faire en consultation avec un bureau public de la protection de la vie privée qui tiendrait également un registre de toutes les associations et compagnies membres.

Commentaires : On trouvera ci-dessous un résumé des points forts et des faiblesses de ce type de méthode :

- Comme dans le modèle d'auto-réglementation, cette méthode ne garantit pas que la majorité des utilisateurs de données adopteront volontairement le système d'enregistrement.
- Elle établit un système de surveillance visant à encourager les compagnies et organismes participants à observer le code. Bien que cette approche puisse avoir beaucoup de poids, elle ne prévoit pas d'autorité formelle en matière d'observation ni d'exécution.
- Elle entraîne des coûts supplémentaires pour les utilisateurs de données.
- Elle offre un niveau de flexibilité élevé et permet à l'industrie et à l'organisme de coordination de s'adapter à l'évolution de la technologie et des pratiques en matière d'information.
- Elle ne garantit pas de droits concrets à l'individu en cas de litige sur l'accès, la correction ou la divulgation. L'organe d'instruction des plaintes des associations professionnelles pourrait cependant jouer un rôle de médiation.
- Bien que l'adoption de différents codes par différents secteurs crée certaines variations au niveau des normes sur la protection de la vie privée, l'organisme de coordination pourrait viser l'uniformité sur les questions importantes comme le droit de l'individu à l'accès, à la correction et à la non-divulgation.

Résumé

On s'est efforcé dans cette section de comparer l'efficacité de plusieurs méthodes qui pourraient être utilisées pour résoudre les problèmes de la protection des renseignements personnels dans le secteur privé. Plutôt que de passer en revue toutes les approches possibles, y compris les systèmes gouvernementaux les plus stricts d'enregistrement et de délivrance de permis, ce document s'est attaché aux méthodes qui semblent convenir davantage à la scène canadienne.

On trouvera à la page suivante un tableau comparatif des quatre méthodes décrites ci-dessus. Les critères utilisés pour les comparaisons sont basés sur l'analyse précédente en fonction du thème majeur de toute discussion sur les choix en matière de réglementation : l'équilibre entre les coûts pour l'industrie et l'établissement de droits individuels ou de mesures de protection pour les citoyens. Les termes "bas", "moyen" et "élevé" cherchent uniquement à donner une idée des valeurs relatives de chaque système.

ÉVALUATION DES SOLUTIONS POSSIBLES

SOLUTIONS

CRITÈRES DE BASE	CODE DE PROTECTION VOLONTAIRE	CODE IMPOSÉ PAR LA LOI	ENREGISTREMENT ET RÉGLEMENTATION	ENREGISTREMENT VOLONTAIRE
Coûts pour l'utilisateur de données	Bas	Bas	Moyens à élevés	Moyens
Flexibilité	Élevée	Moyenne	Moyenne	Élevée
Droit du particulier à l'accès, à la correction et à la non-divulgation	Sans garantie	Droits garantis par version obligatoire de la loi	Droits légaux pour les particuliers	Pas de garantie
Droits du particulier en cas de litige	Aucun	Coûteux et difficile à appliquer pour le particulier	Coûteux à appliquer D'autres systèmes d'enregistrement pourraient pallier ce problème	Aucun
Uniformité des pratiques en matière d'information	Difficile à assurer	Possible dans version obligatoire	Encourage uniformité	Certaine uniformité possible
Efficacité pour le développement de normes générales de protection	Basse à moyenne	Basse à moyenne	Potentiel élevé	Moyenne